

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2003年10月9日 (09.10.2003)

PCT

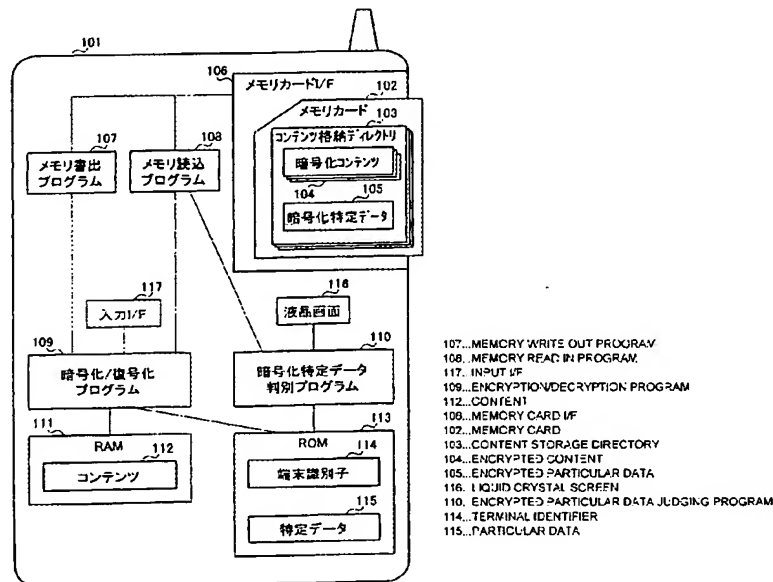
(10) 国際公開番号
WO 03/084125 A1

- (51) 国際特許分類: H04L 9/08, (72) 発明者; および
G11B 20/10, G06F 12/14, H04M 11/00 (75) 発明者/出願人 (米国についてのみ): 中井 信一
(NAKAI, Shinichi) [JP/JP]; 〒226-0024 神奈川県 横浜市 緑区西八朔町138-1-203 Kanagawa (JP). 野口 直彦
(NOGUCHI, Naohiko) [JP/JP]; 〒222-0031 神奈川県 横浜市 港北区太尾町1323-601 Kanagawa (JP). 松居
真一 (MATSUI, Shinichi) [JP/JP]; 〒658-0073 兵庫県 神戸市 東灘区西岡本1-5-16-302 Hyogo (JP). 難波 孝
彰 (NANBA, Takaaki) [JP/JP]; 〒470-0115 愛知県 日進市 南ヶ丘2-4-13 Aichi (JP). 井上 隆司 (INOUE, Ryuji)
[JP/JP]; 〒562-0005 大阪府 箕面市 新稲5-15-B-106 Osaka (JP).
- (21) 国際出願番号: PCT/JP03/02291
- (22) 国際出願日: 2003年2月28日 (28.02.2003)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2002-97429 2002年3月29日 (29.03.2002) JP
- (71) 出願人 (米国を除く全ての指定国について): 松下電
器産業株式会社 (MATSUSHITA ELECTRIC INDUS-
TRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府 門真市
大字門真1006番地 Osaka (JP).
- (74) 代理人: 鷺田 公一 (WASHIDA, Kimihito); 〒206-0034
東京都 多摩市 鶴牧1丁目24-1 新都市センタービル
5階 Tokyo (JP).

[続葉有]

(54) Title: CONTENT PROCESSING DEVICE, CONTENT ACCUMULATION MEDIUM, CONTENT PROCESSING METHOD, AND CONTENT PROCESSING PROGRAM

(54) 発明の名称: コンテンツ処理装置、コンテンツ蓄積媒体、コンテンツ処理方法及びコンテンツ処理プログラム



(57) Abstract: For an encrypted content (104) stored in a content accumulation medium (102), small-data-amount information on the encrypted content (104) is stored in the content accumulation medium (102) in correlation to the encrypted content (104). Thus, without decrypting the large-data-amount encrypted content (104), it is possible to judge the encrypted content (104) according to the small-data-amount information. This enables a user to easily judge a plurality of contents stored in the content accumulation medium.

[続葉有]



(81) 指定国 (国内): CN, JP, US.

添付公開書類:

— 国際調査報告書

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR).

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約: コンテンツ蓄積媒体102に格納された暗号化コンテンツ104について、当該暗号化コンテンツ104に関連したデータ量の少ない情報を当該暗号化コンテンツ104に対応付けてコンテンツ蓄積媒体102に格納することにより、データ量の多い暗号化コンテンツ104を復号化することなく、関連した情報に基づいて暗号化コンテンツ104を判別することができる。これにより、コンテンツ蓄積媒体に格納された複数のコンテンツの判別を一段と容易に行うことができる。

明 細 書

コンテンツ処理装置、コンテンツ蓄積媒体、コンテンツ処理方法及びコンテンツ処理プログラム

5

技術分野

本発明は、コンテンツをコンテンツ蓄積媒体に格納して利用するための、コンテンツ処理装置、コンテンツ蓄積媒体、コンテンツ処理方法及びコンテンツ処理プログラムに関する。

10

背景技術

従来、携帯電話機等の端末装置において、コンテンツプロバイダから各種コンテンツをダウンロードし、これらのコンテンツを当該端末装置において利用するものがある。

15

コンテンツのダウンロードが可能である端末装置は、ダウンロードしたコンテンツを着脱自在の例えばメモ리카ードのようなコンテンツ蓄積媒体に格納することにより、内蔵メモリの容量を大きくすることなく、利用者に複数のコンテンツを提供することが可能となっている。これにより、端末装置の大型化を回避し、可搬性を確保することができる。

20

ところで、コンテンツ蓄積媒体にコンテンツを格納する場合、端末装置は当該コンテンツを所定の暗号化方法によって暗号化した後、これを格納するようになされている。これにより、コンテンツ蓄積媒体に格納されたコンテンツを他の利用環境において利用することを制限している。

また、コンテンツ蓄積媒体は、1つの端末装置だけではなく、複数の端末装置によって、暗号化されたコンテンツを格納することが可能となっている。これにより、利用者は、自分が所有する複数の端末装置においてダウンロードしたコンテンツを1つのメモ리카ードに格納することができる。

25

このように、1つのコンテンツ蓄積媒体には、異なる複数の端末装置によって格納されたコンテンツが混在する場合がある。コンテンツは、端末装置の種類やその構造によって使用可能な対象端末装置が異なっている。

従って、端末装置にコンテンツ蓄積媒体を装着し、当該コンテンツ蓄積媒体
5 からコンテンツを読み出す場合、端末装置は、装着されたコンテンツ蓄積媒体からコンテンツを1つ1つ読み出し、各コンテンツを完全に復号化することによってはじめて当該コンテンツが利用可能であるか否かの判断を行うことが可能となっている。

このように、従来の端末装置においては、コンテンツ蓄積媒体に格納されて
10 いる複数のコンテンツの中から、このとき使用する端末装置において利用可能であるコンテンツを見つけ出す作業として、装着されたコンテンツ蓄積媒体からすべてのコンテンツを1つ1つ読み出し、当該読み出されたコンテンツについて、順次、復号した後に利用可能であるか否かを判断するといった煩雑な作業が必要となり、当該作業にかかる時間が長くなるという問題があった。

また、従来の端末装置においては、コンテンツ蓄積媒体に格納されているコ
15 ンテンツが使用可能であるか否かを判断することが困難な機種もある。このような場合、例えば、コンテンツとしてオーディオデータがコンテンツ蓄積媒体に格納されているとすると、このオーディオデータが端末装置にとって正規のデータでなくとも、その端末装置がこれを再生してしまう可能性があり、大音
20 量が流れる等の不都合が生じる問題があった。

発明の開示

本発明の目的は、コンテンツ蓄積媒体に格納された複数のコンテンツの判別を一段と容易に行うことが可能なコンテンツ処理装置、コンテンツ蓄積媒体、
25 コンテンツ処理方法及びコンテンツ処理プログラムを提供することである。

この目的は、コンテンツ蓄積媒体に格納された暗号化コンテンツについて、当該暗号化コンテンツに関連したデータ量の少ない情報を当該暗号化コンテ

ンツに対応付けてコンテンツ蓄積媒体に格納することにより、データ量の多い暗号化コンテンツを復号化することなく、関連した情報に基づいて暗号化コンテンツを判別することにより達成される。

5 図面の簡単な説明

図 1 は、本発明の実施の形態 1 に係るコンテンツ処理装置の構成を示す外観図、

図 2 は、実施の形態 1 に係るコンテンツ処理装置の構成を示すブロック図、

図 3 は、実施の形態 1 に係るコンテンツ処理装置のコンテンツ書出し処理手順を示すフローチャート、

図 4 は、本発明の実施の形態 1 に係るコンテンツ蓄積媒体のデータ格納状態を示す略線図、

図 5 は、本発明の実施の形態 1 に係るコンテンツ処理装置のコンテンツ読込み処理手順を示すフローチャート、

図 6 は、実施の形態 2 に係るコンテンツ処理装置の構成を示すブロック図、

図 7 は、実施の形態 2 に係るコンテンツ処理装置のコンテンツ書出し処理手順を示すフローチャート、

図 8 は、本発明の実施の形態 2 に係るコンテンツ蓄積媒体のデータ格納状態を示す略線図、

図 9 は、本発明の実施の形態 2 に係るコンテンツ処理装置のコンテンツ読込み処理手順を示すフローチャート、

図 10 は、実施の形態 3 に係るコンテンツ処理装置の構成を示すブロック図、

図 11 は、実施の形態 3 に係るコンテンツ処理装置のコンテンツ書出し処理手順を示すフローチャート、

図 12 は、本発明の実施の形態 3 に係るコンテンツ蓄積媒体のデータ格納状態を示す略線図、

図 13 は、本発明の実施の形態 3 に係るコンテンツ処理装置のコンテンツ読

込み処理手順を示すフローチャート、

図 1 4 は、実施の形態 4 に係るコンテンツ処理装置の構成を示すブロック図、

図 1 5 は、実施の形態 4 に係るコンテンツ処理装置のコンテンツ書出し処理
手順を示すフローチャート、

- 5 図 1 6 は、本発明の実施の形態 4 に係るコンテンツ蓄積媒体のデータ格納状態を示す略線図、

図 1 7 は、本発明の実施の形態 4 に係るコンテンツ処理装置のコンテンツ読み込み処理手順を示すフローチャートは、

図 1 8 は、実施の形態 5 に係るコンテンツ処理装置の構成を示すブロック図、

- 10 図 1 9 は、実施の形態 5 に係るコンテンツ処理装置のコンテンツ書出し処理手順を示すフローチャート、

図 2 0 は、本発明の実施の形態 5 に係るコンテンツ蓄積媒体のデータ格納状態を示す略線図、

- 15 図 2 1 は、本発明の実施の形態 5 に係るコンテンツ処理装置のコンテンツ読み込み処理手順を示すフローチャート、

図 2 2 は、実施の形態 6 に係るコンテンツ処理装置の構成を示すブロック図、

図 2 3 は、実施の形態 6 に係るコンテンツ処理装置のコンテンツ書出し処理
手順を示すフローチャート、

- 20 図 2 4 は、本発明の実施の形態 6 に係るコンテンツ蓄積媒体のデータ格納状態を示す略線図、

図 2 5 は、本発明の実施の形態 6 に係るコンテンツ処理装置のコンテンツ読み込み処理手順を示すフローチャート、

図 2 6 は、実施の形態 7 に係るコンテンツ処理装置の構成を示すブロック図、

- 25 図 2 7 は、実施の形態 7 に係るコンテンツ処理装置のコンテンツ書出し処理手順を示すフローチャート、

図 2 8 は、本発明の実施の形態 7 に係るコンテンツ蓄積媒体のデータ格納状態を示す略線図、及び、

図 29 は、本発明の実施の形態 7 に係るコンテンツ処理装置のコンテンツ読み込み処理手順を示すフローチャートである。

発明を実施するための最良の形態

5 以下、本発明の実施の形態について、図面を参照して詳細に説明する。

（実施の形態 1）

図 1 は、本発明の実施の形態 1 に係るコンテンツ処理装置としての携帯電話機 101 の外観を示す正面図である。

携帯電話機 101 は、携帯電話回線網を介して他の電話機器との間で通話を行う携帯電話機能部に加えて、コンテンツプロバイダから携帯電話回線網を介して音楽またはゲーム等の各種コンテンツをダウンロードするようになって
10 いる。

また、携帯電話機 101 は、コンテンツ蓄積媒体であるカード状の記憶媒体（メモ리카ード 102）を着脱自在とするメモ리카ードインターフェイス（I/F）106 を有し、当該メモ리카ードインターフェイス 106 に装着されたメモ
15 리카ード 102 に対して、携帯電話機 101 の内部メモリに格納されているコンテンツなどの種々の情報を書き込む（以下、これを情報の書出しと称する）とともに、メモ리카ード 102 に格納されているコンテンツなどの種々の情報を読み出す（以下、これを情報の読み込みと称する）ようになっている。

20 携帯電話機 101 の筐体正面部には、操作ボタン等からなる入力インターフェイス（I/F）117 が設けられており、当該入力インターフェイス 117 を利用者が操作することにより、携帯電話機能を利用する際の電話番号等の入力に加えて、コンテンツのダウンロード、メモ리카ード 102 に対する各種情報の書き出し、読み込み等、種々のコマンドを入力することが可能となっている。

25 また、携帯電話機 101 の筐体正面部には、液晶表示部の液晶画面 116 が設けられており、携帯電話機 101 の動作に関する情報、コンテンツの実行に関する各種情報及びコンテンツの内容が表示される。

図 1 との対応部分に同一符号を付して示す図 2 は、携帯電話機 101 の構成を示すブロック図である。この図 2 は、携帯電話機 101 の構成のうち、特にコンテンツ処理に関わる構成を抽出して示すものである。携帯電話機 101 は、それぞれ図示しない CPU (Central Processing Unit) によって動作するメモリ書出プログラム 107、メモリ読込プログラム 108、暗号化/復号化プログラム 109 及び暗号化特定データ判別プログラム 110 を含んでいる。

図 2 において、携帯電話機 101 は、コンテンツプロバイダから携帯電話回線網を介してダウンロードしたコンテンツ 112 を RAM (Random Access Memory) 111 に格納する。暗号化/復号化プログラム 109 は、RAM 111 に格納されたコンテンツ 112 を暗号化するものであり、当該暗号化/復号化プログラム 109 によって暗号化されたコンテンツ 112 は、暗号化コンテンツ 104 として、メモリ書出プログラム 107 によってメモリカードインターフェイス 106 を介してメモリカード 102 に書き込まれる。

ROM (Read Only Memory) 113 は、携帯電話機 101 に固有の、例えば電話番号等なる端末識別子 114 と、この実施の形態に示される、コンテンツをメモリカードに書き込みまたは読み出す処理を行うシステムに共通の、例えば文字列でなる特定データ 115 とを格納している。

暗号化/復号化プログラム 109 は、コンテンツ 112 を暗号化する際、ROM (Read Only Memory) 113 に格納されている端末識別子 114 を用いて暗号化する。また、暗号化/復号化プログラム 109 は、コンテンツ 112 を暗号化してメモリカード 102 に格納する処理に伴って、ROM 113 に格納されている特定データ 115 を端末識別子 114 で暗号化する。当該暗号化の結果である暗号化特定データ 105 は、メモリ書出プログラム 107 によってメモリカード 102 の暗号化コンテンツ 104 と同じディレクトリに格納される。このように、暗号化特定データ 105 を暗号化コンテンツ 104 と同じディレクトリに格納することにより、暗号化特定データ 105 と暗号化コンテンツとが対応付けられた状態でメモリカード 102 に格納される。

また、メモ리카ード102に格納された暗号化コンテンツ104を携帯電話機101に読み込む場合、携帯電話機101のメモリ読込プログラム108は、暗号化コンテンツ104を読み込む処理に先立って、当該暗号化コンテンツ104と同じディレクトリに格納されている暗号化特定データ105をメモ리카ード102からメモ리카ードインターフェイス106を介して読み込む。

当該読み込まれた暗号化特定データ105は、暗号化特定データ判別プログラム110によって復号化される。この場合、暗号化特定データ判別プログラム110は、ROM113に格納されている携帯電話機101に固有の端末識別子114を用いて暗号化特定データを復号化するとともに、当該復号化された特定データとROM113に格納されている特定データ115とを比較し、当該比較結果が一致した場合には、当該復号化したメモ리카ード102の暗号化特定データ105が、携帯電話機101によってメモ리카ード102に書き込まれたものであると判別することができる。

このように、メモ리카ード102に格納されている暗号化特定データ105が、携帯電話機101によってメモ리카ード102に書き込まれたものであることが判ると、暗号化/復号化プログラム109は、当該暗号化特定データ105と同じディレクトリに格納されている暗号化コンテンツ104を復号化し、当該復号化されたコンテンツ112をRAM111に格納する。

図3は、携帯電話機101のRAM111に格納されているコンテンツ112を、メモ리카ード102に格納する際の、暗号化/復号化プログラム109の処理手順を示すフロー図である。

図3に示すように、暗号化/復号化プログラム109は、ステップST201において、ROM113から特定データ115及び端末識別子114を取得する。そして、暗号化/復号化プログラム109は、ステップST202に移って、ステップST201において取得した特定データ115を、ステップST201において取得した携帯電話機101に固有の端末識別子114を用いて、例えばトリプルDES (Data Encryption Standard) 暗号方式によって暗号化す

ることにより、暗号化特定データ105を生成する。

そして、暗号化/復号化プログラム109は、ステップST203に移って、このときメモ리카ードインターフェイス106に装着されているメモ리카ード102に、ステップST202において生成された暗号化特定データ105
5 と同じ暗号化特定データが既に格納されているか否かを判断する。ここで否定結果が得られると、このことは、メモ리카ード102には、携帯電話機101に固有の端末識別子114を用いて暗号化された暗号化特定データ105、すなわち、携帯電話機101によって書き出された暗号化特定データ105が格納されていないことを意味しており、このとき暗号化/復号化プログラム109
10 は、ステップST204に移って、ステップST202において暗号化された暗号化特定データ105を、メモリ書出プログラム107を用いてメモ리카ード102に格納した後、ステップST205に移る。

また、ステップST203において肯定結果が得られると、このことは、メモ리카ード102には、携帯電話機101によって書き出された暗号化特定データ105が格納されていることを意味しており、このとき暗号化/復号化プログラム109は、ステップST205に移る。
15

ステップST205において、暗号化/復号化プログラム109は、RAM111からコンテンツ112を取得した後、ステップST206に移って、ステップST205において取得したコンテンツ112を、ROM113内の端末
20 識別子114を用いて例えばトリプルDES暗号方式で暗号化する。

そして、暗号化/復号化プログラム109は、ステップST207に移って、ステップST206において暗号化された暗号化コンテンツ104を、ステップST204においてメモ리카ード102に格納された暗号化特定データ105と同じディレクトリに格納する。

25 これにより、図4に示すように、メモ리카ード102においては、それぞれ同じ端末識別子114によって暗号化されたコンテンツ112（暗号化コンテンツ104）と特定データ115（暗号化特定データ105）とが、同じディ

レクトリ 301、302 に格納された状態となる。このように、暗号化コンテンツ 104 と暗号化特定データ 105 とを同じディレクトリに格納することにより、これらのデータは対応付けられてメモリカード 102 に格納された状態となる。

- 5 また、図 5 は、図 3 の処理手順によってメモリカード 102 に格納された暗号化コンテンツ 104 と暗号化特定データとを携帯電話機 101 によって読み込んで復号化する際の、暗号化/復号化プログラム 109 と暗号化特定データ判別プログラム 110 との処理手順を示すフロー図である。

- 10 図 5 に示すように、暗号化特定データ判別プログラム 110 は、ステップ S T 401 において、メモリカード 102 内に暗号化特定データ 105 があるかどうかを調べる。ここで否定結果が得られると、このことは、メモリカード 102 には、読み込むべき暗号化特定データ 105 がないこと、すなわち、当該暗号化特定データ 105 に対応付けられた暗号化コンテンツ 104 がないことを意味しており、このとき暗号化特定データ判別プログラム 110 は、この処理手順を終了する。

- 20 これに対して、ステップ S T 401 において肯定結果が得られると、このことは、メモリカード 102 には、読み込むべき暗号化特定データ 105 があること、すなわち、当該暗号化特定データ 105 に対応付けられた暗号化コンテンツ 104 があることを意味しており、このとき暗号化特定データ判別プログラム 110 は、ステップ S T 402 に移って、メモリ読込プログラム 108 を用いてメモリカード 102 から暗号化特定データ 105 を取得した後、ステップ S T 403 に移る。ステップ S T 403 において、暗号化特定データ判別プログラム 110 は、ステップ S T 402 において取得した暗号化特定データ 105 を、ROM 113 に格納されている端末識別子 114 を用いて復号化する。
- 25 そして、暗号化特定データ判別プログラム 110 は、ステップ S T 404 に移って、ステップ S T 403 において復号化された特定データと、ROM 113 に格納されている特定データ 115 とを比較し、復号化された特定データと、

ROM113に格納されている特定データ115とが同一であるか否かを判断する。

因みに、携帯電話機101は、コンテンツ112を暗号化してメモリカード102に書き出す場合には、常に、特定データ115を端末識別子114を用いて暗号化することにより得られる暗号化特定データ105を、暗号化コンテンツ104に対応付けて格納するようになっている。従って、ステップST403において復号化された特定データと、ROM113に格納されている特定データ115との比較結果が一致する場合、このことは、このとき復号化された暗号化特定データ105がその携帯電話機101によってメモリカード102に書き出されたもの、すなわち、当該暗号化特定データ105と対応付けられてメモリカード102に格納されている暗号化コンテンツ104が携帯電話機101によってメモリカード102に書き出されたものであることを意味する。

従って、ステップST403において復号化された特定データと、ROM113に格納されている特定データ115との比較結果が一致する場合、暗号化特定データ判別プログラム110は、当該一致結果を暗号化/復号化プログラム109に通知するとともに、ステップST404からステップST405に移る。

これに対して、ステップST403において復号化された特定データと、ROM113に格納されている特定データ115との比較結果が一致しない場合、暗号化特定データ判別プログラム110は、当該不一致の結果を暗号化/復号化プログラム109に通知するとともに、上述のステップST401に戻って、メモリカード102内に次の暗号化特定データがあるか否かを判断し、次の暗号化特定データがある場合には、その暗号化特定データについて同様の処理を実行する。

ステップST405において、暗号化特定データ判別プログラム110は、上述のステップST404において一致結果が得られた暗号化特定データ105及び当該暗号化特定データ105が格納されているディレクトリ302

に格納されているすべての暗号化特定データを暗号化/復号化プログラム 1 0 9 に復号化させ、その一覧を液晶画面 1 1 6 に表示する。

これにより、液晶画面 1 1 6 には、メモ리카ード 1 0 2 に格納されている暗号化コンテンツのうち、携帯電話機 1 0 1 によって利用可能な暗号化コンテンツ 1 0 4 に対応付けられた特定データ 1 1 5 の一覧が表示される。すなわち、携帯電話機 1 0 1 によって利用可能な暗号化コンテンツ 1 0 4 が、それに対応付けられたデータ量の少ない特定データ 1 1 5 によって一覧表示される。

因みに、この実施の形態においては、暗号化コンテンツ 1 0 4 に対応付けられた暗号化特定データ 1 0 5 を復号化して一覧表示する場合について述べたが、これに限らず、暗号化コンテンツ 1 0 4 を特定データ 1 1 5 に対応付けてメモ리카ード 1 0 2 に格納する際に、その特定データ 1 1 5 に対応したコンテンツのタイトルのみを携帯電話機 1 0 1 の RAM 1 1 1 に格納し、ステップ S T 4 0 4 における特定データ 1 0 5 の一致結果に基づいて、当該格納されているタイトルを一覧表示するようにしてもよい。

ステップ S T 4 0 5 において、液晶画面 1 1 6 にコンテンツの一覧が表示されると、利用者は、入力インターフェイス 1 1 7 を操作することにより、当該表示された一覧のなかから所望とするコンテンツを選択する。

これにより、暗号化/復号化プログラム 1 0 9 は、ステップ S T 4 0 6 に移って、メモリ読込プログラム 1 0 8 を用いて、このとき入力インターフェイス 1 1 7 を介して指定された暗号化コンテンツ 1 0 4 をメモ리카ード 1 0 2 から読み込み、さらに続くステップ S T 4 0 7 に移って、ステップ S T 4 0 6 においてメモ리카ード 1 0 2 から取得した暗号化コンテンツ 1 0 4 を、ROM 1 1 3 に格納されている端末識別子 1 1 4 を用いて復号化し、RAM 1 1 1 に格納する。

RAM 1 1 1 に格納されたコンテンツ 1 1 1 は、携帯電話機 1 0 1 の利用者が入力インターフェイス 1 1 7 を操作することにより起動され、利用者の利用に供される。

以上の構成において、携帯電話機101は、メモ리카ード102に暗号化コンテンツ104を書き出す際に、当該暗号化コンテンツ104に対応付けられた暗号化特定データ105をメモ리카ード102に格納しておく。

この暗号化特定データ105は、例えば、ある文字列を暗号化したものであり、暗号化コンテンツ104に比べてそのデータ量は格段に少ないものとなっている。従って、携帯電話機101は、メモ리카ード102から暗号化コンテンツ104を読み込んで復号化する前に、当該暗号化コンテンツ104に対応付けられた暗号化特定データ105を読み込んでこれを復号化し、当該復号化された特定データが携帯電話機101によってメモ리카ード102に書き出されたものであるか否かを判別する。

復号化された特定データが携帯電話機101によってメモ리카ード102に書き出されたものである場合、当該特定データに対応付けられてメモ리카ード102に格納されている暗号化コンテンツ104も携帯電話機101によってメモ리카ード102に書き出されたものであることになる。

従って、この場合、メモ리카ード102に格納されている暗号化コンテンツ104は、携帯電話機101に読み込んで、当該携帯電話機101によって利用することが可能であり、携帯電話機101の暗号化/復号化プログラム109は、メモ리카ード102から暗号化コンテンツ104を読み込み、当該読み込まれた暗号化コンテンツ104を復号化する。

このように、暗号化特定データ105の復号結果が、ROM113に格納されている特定データ115と一致することを条件に、当該暗号化特定データ105に対応付けられた暗号化コンテンツ104をメモ리카ード102から携帯電話機101に読み込んで復号化することにより、携帯電話機101は、当該携帯電話機101において利用可能である暗号化コンテンツ104のみを選択的に復号化することができる。

従って、メモ리카ード102に複数の暗号化コンテンツが格納されている状態であって、これら複数の暗号化コンテンツを利用可能な端末装置（携帯電話

機等) が各暗号化コンテンツ毎に異なる場合であっても、携帯電話機 101 は、これら複数のデータ量の多い暗号化コンテンツをすべて復号化する必要はなく、当該複数の暗号化コンテンツにそれぞれ対応付けられた、データ量の少ない暗号化特定データを復号化するだけで、利用可能な暗号化コンテンツ 104 を判別することができる。

このように、本実施の形態のコンテンツ処理装置としての携帯電話機 101 によれば、コンテンツ蓄積媒体であるメモリカード 102 に格納された複数の暗号化コンテンツの判別を一段と容易に行うことが可能となり、携帯電話機 101 において利用可能な暗号化コンテンツ 104 を一段と迅速に復号化することができる。

なお、この実施の形態の携帯電話機 101 においては、端末識別子 114 として、その携帯電話機 101 の電話番号を用いる場合について述べたが、これに限らず、例えば携帯電話機 101 の製造番号のようなその携帯電話機 101 を識別するための識別子、又は、その他の何らかの意味を持つ文字列、数値、画像または音声等のデータ、若しくは特定のサービスと契約したことを示す識別子（会員番号等）を用いるようにしてもよい。また、この端末識別子 114 として電話番号、製造番号、又はその他の文字列等の情報そのものではなく、端末識別子に対してある変換を加えた結果（端末識別子に関連する情報）を用いるようにしてもよい。このようにすれば、端末識別子によってコンテンツ及び特定データを暗号化する際の暗号化方法、及び端末識別子が第三者に漏洩した場合であっても、その端末識別子は、暗号化鍵となり得る他のデータに変換されていることにより、このデータ（暗号化鍵）によって暗号化された暗号化コンテンツ及び暗号化特定データが解読されることを防止することができる。

また、この実施の形態の携帯電話機 101 においては、特定データ 115 として、コンテンツをメモリカードに書き込みまたは読み出す処理を行うシステムに共通の、例えば文字列を用いる場合について述べたが、これに限らず、端末識別子として設定されている情報とは異なる他の識別子（例えば端末識別子

1 1 4として電話番号が設定されている場合は、特定データとして製造番号)、その他の何らかの意味を持つ文字列、数値、画像または音声等のデータ、若しくは特定のサービスと契約したことを示す識別子(会員番号等)を用いるようにしてもよい。

- 5 また、この実施の形態においては、コンテンツを格納するコンテンツ蓄積媒体としてメモリカード1 0 2を用いる場合について述べたが、これに限らず、要はデジタル情報化されたコンテンツを格納可能なコンテンツ蓄積媒体であれば、他のデバイスを広く適用することができる。

(実施の形態2)

- 10 図6は、本発明の実施の形態2に係るコンテンツ処理装置としての携帯電話機5 0 1の構成を示すブロック図である。但し、図1及び図2と同一の構成となるものについては、図1及び図2と同一番号を付し、詳しい説明を省略する。

この図6に示される携帯電話機5 0 1は、認証プログラム5 1 0を有し、当該認証プログラム5 1 0によって認証を行うことによりアクセスが可能となる認証領域5 0 4をメモリカード5 0 2に設け、当該認証領域5 0 4に暗号化
15 特定データ5 0 4を格納するようにした点が図2の構成の携帯電話機1 0 1と異なる。

- 図2との対応部分に同一符号を付して示す図6は、携帯電話機5 0 1の構成を示すブロック図である。この図6は、携帯電話機5 0 1の構成のうち、特に
20 コンテンツ処理に関わる構成を抽出して示すものである。携帯電話機5 0 1は、それぞれ図示しないCPU(Central Processing Unit)によって動作するメモリ書出プログラム1 0 7、メモリ読込プログラム1 0 8、暗号化/復号化プログラム5 1 3、暗号化特定データ判別プログラム5 1 4及び認証プログラム5 1 0を含んでいる。

- 25 図6において、携帯電話機5 0 1は、コンテンツプロバイダから携帯電話回線網を介してダウンロードしたコンテンツ5 1 6をRAM(Random Access Memory)5 1 5に格納する。暗号化/復号化プログラム5 1 3は、RAM5 1

5に格納されたコンテンツ516を暗号化するものであり、当該暗号化/復号化プログラム513によって暗号化されたコンテンツ516は、暗号化コンテンツ507として、メモリ書出プログラム107によってメモ리카ードインターフェイス106を介してメモ리카ード502の通常領域505に書き込まれる。通常領域505は、携帯電話機501に設けられた認証プログラム510の認証を必要とせずにアクセス可能な領域である。

ROM (Read Only Memory) 517は、携帯電話機501に固有の、例えば電話番号等なる端末識別子518と、この実施の形態に示されるコンテンツをメモ리카ードに書き込み、または読み出す処理を行うシステムに共通の、
10 例えば文字列でなる特定データ519とを格納している。

暗号化/復号化プログラム513は、コンテンツ516を暗号化する際、ROM (Read Only Memory) 517に格納されている端末識別子518を用いて暗号化する。また、暗号化/復号化プログラム513は、コンテンツ516を暗号化してメモ리카ード502に格納する処理に伴って、ROM517に格納されてい
15 る特定データ519を端末識別子518で暗号化する。当該暗号化の結果である暗号化特定データ504は、メモリ書出プログラム107によってメモ리카ード502の認証領域503に格納される。この認証領域503における暗号化特定データ504は、通常領域505の暗号化コンテンツ507が格納されるディレクトリと同じディレクトリに格納されるリンク情報508によ
20 って暗号化コンテンツ507と対応付けられる。このように、暗号化特定データ504及び暗号化コンテンツ507は、リンク情報508によって対応付けられて、認証領域503及び通常領域505に分けて格納される。

また、メモ리카ード502に格納された暗号化コンテンツ507を携帯電話機501に読み込む場合、携帯電話機501のメモリ読込プログラム108は、
25 暗号化コンテンツ507を読み込む処理に先立って、当該暗号化コンテンツ507と同じディレクトリに格納されているリンク情報508によって対応付けられた、認証領域503の暗号化特定データ504をメモ리카ード502か

らメモ리카ードインターフェイス106を介して読み込む。

当該読み込まれた暗号化特定データ504は、暗号化特定データ判別プログラム514によって復号化される。この場合、暗号化特定データ判別プログラム514は、ROM517に格納されている携帯電話機501に固有の端末識別子518を用いて暗号化特定データ504を復号化することにより、当該復号化された特定データとROM517に格納されている特定データ519とが一致した場合には、当該復号化したメモ리카ード502の暗号化特定データ504が、携帯電話機501によってメモ리카ード502に書き込まれたものであると判別することができる。

10 このように、メモ리카ード502に格納されている暗号化特定データ504が、携帯電話機501によってメモ리카ード502に書き込まれたものであることが判ると、暗号化/復号化プログラム513は、当該暗号化特定データ504に対応付けられた、通常領域505の暗号化コンテンツ507を復号化し、当該復号化されたコンテンツ516をRAM515に格納する。

15 図7は、携帯電話機501のRAM516に格納されているコンテンツ516を、メモ리카ード502に格納する際の、認証プログラム510及び暗号化/復号化プログラム513の処理手順を示すフロー図である。

図7に示すように、認証プログラム510は、ステップST601において、まず、メモ리카ード502との間で認証を行う。因みに、メモ리카ード502
20 には、図示しない認証プログラムが設けられており、携帯電話機501の認証プログラム510との間で認証処理を行い、当該認証結果として携帯電話機501がメモ리카ード502の認証領域503にアクセス可能である端末装置であるという結果が得られると、認証領域503へのアクセスを許可するようになされている。

25 ステップST601における認証処理の結果として、携帯電話機501からメモ리카ード502の認証領域503へのアクセスが可能になると、認証プログラム510は、当該認証結果を暗号化/復号化プログラム513に通知する。

この通知を受け取った暗号化/復号化プログラム513は、ステップST602において、ROM517から特定データ519を取得する。そして、暗号化/復号化プログラム513は、ステップST603に移って、ステップST602において取得した特定データ519を、ROM517に格納されている、携帯5
5 帯電話機501に固有の端末識別子518を用いて、例えばトリプルDES暗号方式によって暗号化することにより、暗号化特定データ504を生成する。

そして、暗号化/復号化プログラム513は、ステップST604に移って、このときメモ리카ードインターフェイス106に装着されているメモ리카ード502の認証領域503に、ステップST603において生成された暗号化
10 特定データ504と同じ暗号化特定データが既に格納されているか否かを判断する。ここで否定結果が得られると、このことは、メモ리카ード502には、携帯5
帯電話機501に固有の端末識別子518を用いて暗号化された暗号化特定データ504、すなわち、携帯5
帯電話機501によって書き出された暗号化特定データ504が格納されていないことを意味しており、このとき暗号化/復号
15 化プログラム513は、ステップST605に移って、ステップST603において暗号化された暗号化特定データ504とリンク情報508を、メモリ書
出プログラム107を用いてメモ리카ード502に格納した後、ステップST
606に移る。この場合、暗号化/復号化プログラム513は、暗号化特定データ504を認証領域503に格納するとともに、リンク情報508を通常領域
20 505のコンテンツ格納ディレクトリ506に格納する。リンク情報508は、認証領域503に格納された暗号化特定データ504と、これに対応付けられ
た、通常領域505の暗号化コンテンツ507とを対応付けるための情報である。

また、ステップST604において肯定結果が得られると、このことは、メモ
25 リカード502には、携帯5
帯電話機501によって書き出された暗号化特定データ504が格納されていることを意味しており、このとき暗号化/復号化プログラム513は、ステップST606に移る。

ステップST606において、暗号化/復号化プログラム513は、RAM515からコンテンツ516を取得した後、ステップST607に移って、ステップST606において取得したコンテンツ516を、ROM517内の端末識別子518を用いて例えばトリプルDES暗号方式で暗号化する。

- 5 そして、暗号化/復号化プログラム513は、ステップST608に移って、ステップST607において暗号化された暗号化コンテンツ507を、ステップST605においてメモ리카ード502に格納された暗号化特定データ504とリンク情報508によって対応付けられたディレクトリに格納する。

- 10 これにより、図8に示すように、メモ리카ード502においては、それぞれ同じ端末識別子518によって暗号化されたコンテンツ516（暗号化コンテンツ507）と特定データ519（暗号化特定データ504）とが、リンク情報508によって対応付けられて格納された状態となる。このように、暗号化コンテンツ507と暗号化特定データ504とをリンク情報508によって対応付けるとともに、暗号化コンテンツ507の存在を確認するための暗号化
- 15 特定データ504を認証領域503に格納することにより、認証領域503にアクセスが可能な携帯電話機501のみによって暗号化コンテンツ507の存在を確認することが可能な状態となる。

- 20 また、図9は、図7の処理手順によってメモ리카ード502に格納された暗号化コンテンツ507と暗号化特定データ504とを携帯電話機501によって読み込んで復号化する際の、暗号化/復号化プログラム513と暗号化特定データ判別プログラム514との処理手順を示すフロー図である。

- 25 図9に示すように、暗号化特定データ判別プログラム514は、ステップST701において、メモ리카ード502の通常領域505にリンク情報508があるか否かを判断する。ここで否定結果が得られると、このことは、リンク情報508がメモ리카ード502に格納されていないこと、すなわち、暗号化コンテンツ507が格納されていないことを意味しており、このとき暗号化特定データ判別プログラム514は、当該処理手順を終了する。

これに対して、ステップST701において肯定結果が得られると、このことは、リンク情報508がメモ리카ード502に格納されていること、すなわち、暗号化コンテンツ507が存在することを意味しており、このとき、暗号化特定データ判別プログラム514は、ステップST702に移って、認証プログラム510による認証処理を行った上で、メモリ読込プログラム108を用いてメモ리카ード502から、リンク情報508に対応する暗号化特定データ504を認証領域503から取得する。

そして、暗号化特定データ判別プログラム514は、ステップST703に移って、ステップST702において取得した暗号化特定データ504を、ROM517に格納されている端末識別子518を用いて復号化する。

そして、暗号化特定データ判別プログラム514は、ステップST704に移って、ステップST703において復号化された特定データと、ROM517に格納されている特定データ519とを比較し、復号化された特定データと、ROM517に格納されている特定データ519とが同一であるか否かを判断する。

因みに、携帯電話機501は、コンテンツ516を暗号化してメモ리카ード502に書き出す場合には、常に、特定データ519を端末識別子518を用いて暗号化することにより得られる暗号化特定データ504を、暗号化コンテンツ507に対応付けて格納するようになっている。従って、ステップST703において復号化された特定データと、ROM517に格納されている特定データ519との比較結果が一致する場合、このことは、このとき復号化された暗号化特定データ504が携帯電話機501によってメモ리카ード502に書き出されたもの、すなわち、当該暗号化特定データ504とリンク情報508によって対応付けられてメモ리카ード502に格納されている暗号化コンテンツ507が携帯電話機501によってメモ리카ード502に書き出されたものであることを意味する。

従って、ステップST703において復号化された特定データと、ROM5

17に格納されている特定データ519との比較結果が一致する場合、暗号化特定データ判別プログラム514は、当該一致結果を暗号化/復号化プログラム513に通知するとともに、ステップST704からステップST705に移る。

これに対して、ステップST703において復号化された特定データと、ROM517に格納されている特定データ519との比較結果が一致しない場合、暗号化特定データ判別プログラム514は、当該不一致の結果を暗号化/復号化プログラム513に通知するとともに、上述のステップST701に戻って、メモ리카ード502内に次のリンク情報508があるか否かを判断し、次のリンク情報508がある場合には、そのリンク情報508について同様の
10 処理を実行する。

ステップST705において、暗号化特定データ判別プログラム514は、上述のステップST704において一致結果が得られた特定データ519の一覧を液晶画面116に表示する。すなわち、携帯電話機501によって利用可能な暗号化コンテンツ507が、それに対応付けられたデータ量の少ない特定データ519によって一覧表示される。
15

因みに、この実施の形態においては、暗号化コンテンツ507に対応付けられた暗号化特定データ504を復号化して一覧表示する場合について述べたが、これに限らず、暗号化コンテンツ507を特定データ516に対応付けてメモ리카ード502に格納する際に、その特定データ516に対応したコンテンツのタイトルのみを携帯電話機501のRAM515に格納し、ステップST704における特定データ519の一致結果に基づいて、当該格納されているタイトルを一覧表示するようにしてもよい。
20

ステップST705において、液晶画面116にコンテンツの一覧が表示されると、利用者は、入力インターフェイス117を操作することにより、当該表示された一覧のなかから所望とするコンテンツを選択する。
25

これにより、暗号化/復号化プログラム513は、ステップST706に移って、メモリ読込プログラム108を用いて、このとき入力インターフェイス1

17を介して指定された暗号化コンテンツ507をメモ리카ード502から読み込み、さらに続くステップST707に移って、ステップST706においてメモ리카ード502から取得した暗号化コンテンツ507を、ROM517に格納されている端末識別子518を用いて復号化し、RAM515に格納5 する。

RAM515に格納されたコンテンツ516は、携帯電話機501の利用者が入力インターフェイス117を操作することにより起動され、利用者の利用に供される。

以上の構成において、携帯電話機501は、メモ리카ード502に暗号化コンテンツ507を書き出す際に、当該暗号化コンテンツ507に対応付けられた暗号化特定データ504をメモ리카ード502の認証領域503に格納しておく。

この暗号化特定データ504は、例えば、ある文字列を暗号化したものであり、暗号化コンテンツ507に比べてそのデータ量は格段に少ないものとなっている。従って、携帯電話機501は、メモ리카ード502から暗号化コンテンツ507を読み込んで復号化する前に、当該暗号化コンテンツ507に対応付けられた暗号化特定データ504を読み込んでこれを復号化し、当該復号化された特定データが携帯電話機501によってメモ리카ード502に書き出されたものであるか否かを判別することにより、データ量の少ない特定データ20 に基づいて、携帯電話機501において利用可能なコンテンツがメモ리카ード502に存在するか否かを容易に判断することができる。

この実施の形態の場合、暗号化特定データ504は、認証領域503に格納されていることにより、携帯電話機501からメモ리카ード502の認証領域503へのアクセスは、認証処理を行った上で実行される。従って、認証領域25 503へのアクセスが可能な携帯電話機501以外の端末装置では、暗号化特定データ504の取得が困難となることにより、利用可能である暗号化コンテンツの判別を容易に行うことは困難となる。

このように、本実施の形態のコンテンツ処理装置としての携帯電話機 501 によれば、コンテンツ蓄積媒体であるメモリカード 502 に格納された複数の暗号化コンテンツの判別を、認証が可能な携帯電話機 501 においてのみ一段と容易に行うことが可能となる。

- 5 なお、この実施の形態の携帯電話機 501 においては、端末識別子 518 として、その携帯電話機 501 の電話番号を用いる場合について述べたが、これに限らず、例えば携帯電話機 501 の製造番号のようなその携帯電話機 501 を識別するための識別子、又は、その他の何らかの意味を持つ文字列、数値、画像または音声等のデータ、若しくは特定のサービスと契約したことを示す識別子（会員番号等）を用いるようにしてもよい。また、この端末識別子 518
- 10 として電話番号、製造番号、又はその他の文字列等の情報そのものではなく、端末識別子に対してある変換を加えた結果（端末識別子に関連する情報）を用いるようにしてもよい。このようにすれば、端末識別子によってコンテンツ及び特定データを暗号化する際の暗号化方法、及び端末識別子が第三者に漏洩し
- 15 た場合であっても、その端末識別子は、暗号化鍵となり得る他のデータに変換されていることにより、このデータ（暗号化鍵）によって暗号化された暗号化コンテンツ及び暗号化特定データが解読されることを防止することができる。

- また、この実施の形態の携帯電話機 501 においては、特定データ 519 として、コンテンツをメモリカードに書き込みまたは読み出す処理を行うシステムに共通の、例えば文字列を用いる場合について述べたが、これに限らず、端
- 20 末識別子として設定されている情報とは異なる他の識別子（例えば端末識別子 518 として電話番号が設定されている場合は、特定データとして製造番号）、その他の何らかの意味を持つ文字列、数値、画像または音声等のデータ、若しくは特定のサービスと契約したことを示す識別子（会員番号等）を用いるよう
- 25 にしてもよい。

また、この実施の形態においては、通常領域に格納されたリンク情報によって認証領域の暗号化特定データを特定する場合について述べたが、これに限ら

ず、例えば、通常領域に格納されている暗号化コンテンツの当該通常領域での格納位置を示す情報（ルート名、ディレクトリ名等）と、これに対応して認証領域に格納されている暗号化特定データの当該認証領域での格納位置を示す情報（ルート名、ディレクトリ名等）を同一とするようにしてもよい。このよう

5 うに同じディレクトリ構成とすれば、リンク情報を用いることなく認証領域での暗号化特定データと通常領域の暗号化コンテンツとを対応付けることができる。

また、この実施の形態においては、コンテンツを格納するコンテンツ蓄積媒体としてメモリカード502を用いる場合について述べたが、これに限らず、

10 要はデジタル情報化されたコンテンツを格納可能なコンテンツ蓄積媒体であれば、他のデバイスを広く適用することができる。

（実施の形態3）

図10は、本発明の実施の形態3に係るコンテンツ処理装置としての携帯電話機901の構成を示すブロック図である。但し、図1及び図2と同一の構成

15 となるものについては、図1及び図2と同一番号を付し、詳しい説明を省略する。

この図10に示される携帯電話機901は、ROM913に格納される端末識別子914として、メモリカード902における暗号化コンテンツ905を格納するディレクトリ名とし、当該ディレクトリ名を特定データ115（図2）

20 の代わりとして用いるようにした点が図2の構成の携帯電話機101と異なる。

図2との対応部分に同一符号を付して示す図10は、携帯電話機901の構成を示すブロック図である。この図10は、携帯電話機901の構成のうち、特にコンテンツ処理に関わる構成を抽出して示すものである。携帯電話機90

25 1は、それぞれ図示しないCPU（Central Processing Unit）によって動作するメモリ書出プログラム107、メモリ読込プログラム108、暗号化/復号化プログラム909及びコンテンツ格納ディレクトリ判別プログラム910を

含んでいる。

図10において、携帯電話機901は、コンテンツプロバイダから携帯電話回線網を介してダウンロードしたコンテンツ912をRAM(Random Access Memory)911に格納する。暗号化/復号化プログラム909は、RAM911に格納されたコンテンツ912を暗号化するものであり、当該暗号化/復号化プログラム909によって暗号化されたコンテンツ912は、暗号化コンテンツ905として、メモリ書出プログラム107によってメモ리카ードインターフェイス106を介してメモ리카ード902に書き込まれる。

ROM(Read Only Memory)913は、携帯電話機901に固有の所定の文字列でなる識別子であって、暗号化コンテンツをメモ리카ード902に格納する際に用いられるディレクトリ名904となる端末識別子914を格納している。

暗号化/復号化プログラム909は、コンテンツ912を暗号化する際、ROM(Read Only Memory)913に格納されている端末識別子914を用いて暗号化する。また、暗号化/復号化プログラム909は、当該暗号化されたコンテンツ912(暗号化コンテンツ905)をメモ리카ード902に格納する際、当該格納先となるコンテンツ格納ディレクトリ(以下、これを単にディレクトリと称する)903のディレクトリ名904を、ROM913に格納されている端末識別子914とする。

また、メモ리카ード902に格納された暗号化コンテンツ905を携帯電話機901に読み込む場合、携帯電話機901のメモリ読込プログラム108は、暗号化コンテンツ905を読み込む処理に先立って、当該暗号化コンテンツ905が格納されているディレクトリ名をメモ리카ード902から取得し、当該取得されたディレクトリ名とROM913に格納されている端末識別子914とが一致した場合には、当該取得したメモ리카ード902のディレクトリ名が、携帯電話機901によってメモ리카ード902に設定されたものであると判別することができる。

このように、メモリカード902に設定されているディレクトリ名が、携帯電話機901によってメモリカード902に設定されたものであることが判ると、暗号化/復号化プログラム909は、当該ディレクトリ名904が設定されたディレクトリ903に格納されている暗号化コンテンツ905を復号化

5 し、当該復号化されたコンテンツ912をRAM911に格納する。

図11は、携帯電話機901のRAM911に格納されているコンテンツ912を、メモリカード902に格納する際の、暗号化/復号化プログラム909の処理手順を示すフロー図である。

図11に示すように、暗号化/復号化プログラム909は、ステップST1001において、ROM913から端末識別子914を取得する。そして、暗号化/復号化プログラム909は、ステップST1002に移って、ステップST1001において取得した端末識別子名のディレクトリ903がメモリカード902にあるか否かを判断する。

ここで否定結果が得られると、このことは、メモリカード902には、携帯電話機901によって設定されたディレクトリ903が存在しないことを意味しており、このとき、暗号化/復号化プログラム909は、ステップST1003に移って、ROM913に格納されている端末識別子名のディレクトリ903を作成し、ステップST1004に移る。

これに対して、ステップST1002において肯定結果が得られると、このことは、既に携帯電話機901によって作成されたディレクトリ903がメモリカード902に存在することを意味しており、このとき暗号化/復号化プログラム909はステップST1004に移る。

ステップST1004において、暗号化/復号化プログラム909は、RAM911からコンテンツ912を取得した後、ステップST1005に移って、
25 ステップST1004において取得したコンテンツ912を、ROM113内の端末識別子914を用いて例えばトリプルDES暗号方式で暗号化する。

そして、暗号化/復号化プログラム909は、ステップST1006に移って、

ステップST1005において暗号化された暗号化コンテンツ905を、ステップST1003において作成されたディレクトリ903に格納する。

これにより、図12に示すように、メモ리카ード902においては、それぞれ同じ端末識別子914によって暗号化されたコンテンツ912（暗号化コンテンツ905）、すなわち一つの携帯電話機901によって書き出された暗号化コンテンツ905が、当該携帯電話機固有の端末識別子名のディレクトリ903に格納された状態となる。

また、図13は、図11の処理手順によってメモ리카ード902に格納された暗号化コンテンツ905を携帯電話機901によって読み込んで復号化する際の、暗号化/復号化プログラム909とコンテンツ格納ディレクトリ判別プログラム910との処理手順を示すフロー図である。

図13に示すように、コンテンツ格納ディレクトリ判別プログラム910は、ステップST1201において、メモ리카ード902内にディレクトリがあるか否かを調べる。ここで否定結果が得られると、このことは、メモ리카ード902には、読み込むべき暗号化コンテンツ905がないことを意味しており、このときコンテンツ格納ディレクトリ判別プログラム910は、この処理手順を終了する。

これに対して、ステップST1201において肯定結果が得られると、このことは、メモ리카ード902には、読み込むべき暗号化コンテンツ905があることを意味しており、このときコンテンツ格納ディレクトリ判別プログラム910は、ステップST1202に移って、メモリ読込プログラム108を用いてメモ리카ード902からディレクトリ名を取得した後、ステップST1203に移る。ステップST1203において、コンテンツ格納ディレクトリ判別プログラム910は、ステップST1202において取得したディレクトリ名が、ROM913に格納されている端末識別子914と同一であるか否かを判断する。

ここで否定結果が得られると、このことは、このときメモ리카ード902か

ら取得したディレクトリ名が、携帯電話機901によって設定されたディレクトリ904ではないこと、すなわち、そのディレクトリに格納されている暗号化コンテンツは、携帯電話機901によって利用できないものであることを意味しており、このとき、コンテンツ格納ディレクトリ判別プログラム910は、

5 当該不一致の結果を暗号化/復号化プログラム909に通知するとともに、上述のステップST1201に戻って、メモ리카ード902内に次のディレクトリがあるか否かを判断し、次のディレクトリがある場合には、そのディレクトリについて同様の処理を実行する。

これに対して、ステップST1203において肯定結果が得られると、この

10 ことは、このとき取得したディレクトリが、携帯電話機901によって設定されたもの、すなわち、そのディレクトリに格納されている暗号化コンテンツは、携帯電話機901によって利用できるものであることを意味しており、このとき、コンテンツ格納ディレクトリ判別プログラム910は、当該一致の結果を暗号化/復号化プログラム909に通知するとともに、ステップST1204に

15 移る。

ステップST1204において、コンテンツ格納ディレクトリ判別プログラム910は、上述のステップST1203において一致結果が得られたディレクトリ904の情報、または当該ディレクトリに格納されている暗号化コンテンツ905に関する情報（例えばタイトル等）を、液晶画面116に一覧表示

20 する。

これにより、液晶画面116には、メモ리카ード902に格納されている暗号化コンテンツのうち、携帯電話機901によって利用可能な暗号化コンテンツ905に関連する情報が表示される。

因みに、携帯電話機901によって利用可能な暗号化コンテンツ905に関する情報を一覧表示する構成としては、暗号化コンテンツ905をメモ리카ード902に格納する際に、その暗号化コンテンツ905に対応したタイトル等の簡易情報のみを携帯電話機901のRAM911に格納し、ステップST1

25

203における一致結果に基づいて、当該格納されている簡易情報を一覧表示する等の方法も考えられる。

- ステップST1204において、液晶画面116にコンテンツの一覧が表示されると、利用者は、入力インターフェイス117を操作することにより、当
- 5 該表示された一覧のなかから所望とするコンテンツを選択する。

- これにより、暗号化/復号化プログラム909は、ステップST1205に移って、メモリ読込プログラム108を用いて、このとき入力インターフェイス117を介して指定された暗号化コンテンツ905をメモ리카ード902から読み込み、さらに続くステップST1206に移って、ステップST120
- 10 5においてメモ리카ード902から取得した暗号化コンテンツ905を、ROM913に格納されている端末識別子914を用いて復号化し、RAM911に格納する。

- RAM911に格納されたコンテンツ912は、携帯電話機901の利用者が入力インターフェイス117を操作することにより起動され、利用者の利用
- 15 に供される。

以上の構成において、携帯電話機901は、メモ리카ード902に暗号化コンテンツ905を書き出す際に、当該暗号化コンテンツ905を格納するディレクトリ904の名前として、当該携帯電話機901に固有の端末識別子914を用いる。

- 20 このディレクトリ名は、暗号化コンテンツ905に比べてそのデータ量は格段に少ないものとなっている。従って、携帯電話機901は、メモ리카ード902から暗号化コンテンツ905を読み込んで復号化する前に、当該暗号化コンテンツ905が格納されたディレクトリ904のディレクトリ名を読み込んで、当該ディレクトリ名が携帯電話機901の端末識別子914と一致する
- 25 か否かを判別する。

ディレクトリ名が携帯電話機901の端末識別子914と一致する場合、当該ディレクトリ名が付けられたディレクトリ904に格納されている暗号化

コンテンツ 905 は、携帯電話機 901 によってメモ리카ード 902 に書き出されたものであることになる。

従って、この暗号化コンテンツ 905 は、携帯電話機 901 に読み込んで、当該携帯電話機 901 によって利用することが可能であり、携帯電話機 901
5 の暗号化/復号化プログラム 909 は、メモ리카ード 902 から暗号化コンテンツ 905 を読み込み、当該読み込まれた暗号化コンテンツ 905 を復号化する。

このように、ディレクトリ名が、ROM 913 に格納されている端末識別子 914 と一致することを条件に、当該ディレクトリ名が付けられたディレクトリ 904 に格納されている暗号化コンテンツ 905 をメモ리카ード 902 から
10 携帯電話機 901 に読み込んで復号化することにより、携帯電話機 901 は、当該携帯電話機 901 において利用可能である暗号化コンテンツ 905 のみを選択的に復号化することができる。

従って、メモ리카ード 902 に複数の暗号化コンテンツが格納されている状態であって、これら複数の暗号化コンテンツを利用可能な端末装置（携帯電話
15 機等）が各暗号化コンテンツ毎に異なる場合であっても、携帯電話機 901 は、これら複数のデータ量の多い暗号化コンテンツをすべて復号化する必要はなく、当該複数の暗号化コンテンツにそれぞれ対応付けられた、データ量の少ないディレクトリを取得するだけで、利用可能な暗号化コンテンツ 905 を判別することができる。

20 このように、本実施の形態のコンテンツ処理装置としての携帯電話機 901 によれば、コンテンツ蓄積媒体であるメモ리카ード 902 に格納された複数の暗号化コンテンツの判別を一段と容易に行うことが可能となり、携帯電話機 901 において利用可能な暗号化コンテンツ 905 を一段と迅速に復号化することができる。また、本実施の形態のコンテンツ処理装置としての携帯電話機
25 901 によれば、ROM 913 に格納された端末識別子 914 をそのままメモ리카ード 902 のディレクトリ名として用いることにより、一段と簡単な構成によって暗号化コンテンツ 905 の判別を行うことができる。

なお、この実施の形態においては、コンテンツを格納するコンテンツ蓄積媒体としてメモ리카ード902を用いる場合について述べたが、これに限らず、要はデジタル情報化されたコンテンツを格納可能なコンテンツ蓄積媒体であれば、他のデバイスを広く適用することができる。

5 (実施の形態4)

図14は、本発明の実施の形態4に係るコンテンツ処理装置としての携帯電話機1301の構成を示すブロック図である。但し、図1及び図2と同一の構成となるものについては、図1及び図2と同一番号を付し、詳しい説明を省略する。

10 この図14に示される携帯電話機1301は、認証プログラム1309を有し、当該認証プログラム1309によって認証を行うことによりアクセスが可能となる認証領域1303をメモ리카ード1302に設け、当該認証領域1303に端末装置（携帯電話機1301）に固有の端末識別子1317を格納するようにした点が図2の構成の携帯電話機101と異なる。

15 図2との対応部分に同一符号を付して示す図14は、携帯電話機1301の構成を示すブロック図である。この図14は、携帯電話機1301の構成のうち、特にコンテンツ処理に関わる構成を抽出して示すものである。携帯電話機1301は、それぞれ図示しないCPU（Central Processing Unit）によって動作するメモリ書出プログラム107、メモリ読込プログラム108、暗号化/復号化プログラム1312、コンテンツ格納ディレクトリ判別プログラム1313及び認証プログラム1309を含んでいる。

図14において、携帯電話機1301は、コンテンツプロバイダから携帯電話回線網を介してダウンロードしたコンテンツ1315をRAM（Random Access Memory）1314に格納する。暗号化/復号化プログラム1312は、
25 RAM1314に格納されたコンテンツ1315を暗号化するものであり、当該暗号化/復号化プログラム1312によって暗号化されたコンテンツ1315は、暗号化コンテンツ1307として、メモリ書出プログラム107によっ

てメモリカードインターフェイス106を介してメモリカード1302の通常領域1305に書き込まれる。通常領域1305は、携帯電話機1301に設けられた認証プログラム1309の認証処理を必要とせずにアクセス可能な領域である。

- 5 ROM (Read Only Memory) 1316は、携帯電話機1301に固有の、例えば電話番号等となる端末識別子1317を格納している。

- 暗号化/復号化プログラム1312は、コンテンツ1315を暗号化する際、ROM (Read Only Memory) 1316に格納されている端末識別子1317を用いて暗号化する。また、暗号化/復号化プログラム1312は、コンテンツ
- 10 1315を暗号化してメモリカード1302に格納する処理に伴って、ROM 1316に格納されている端末識別子1317を、メモリ書出プログラム107によってメモリカード1302の認証領域1303に格納する。この認証領域1303における端末識別子1317は、通常領域1305の暗号化コンテンツ1307が格納されるディレクトリと同じディレクトリに格納されるリンク情報1308によって暗号化コンテンツ1307と対応付けられる。この
- 15 ように、端末識別子1317及び暗号化コンテンツ1307は、リンク情報1308によって対応付けられて、認証領域1303及び通常領域1305に分けて格納される。

- また、メモリカード1302に格納された暗号化コンテンツ1307を携帯電話機1301に読み込む場合、携帯電話機1301のメモリ読込プログラム
- 20 108は、暗号化コンテンツ1307を読み込む処理に先立って、当該暗号化コンテンツ1307と同じディレクトリに格納されているリンク情報1308によって対応付けられた、認証領域1303の端末識別子1317をメモリカード1302からメモリカードインターフェイス106を介して読み込む。
- 25 当該読み込まれた端末識別子1317は、コンテンツ格納ディレクトリ判別プログラム1313によって、ROM1316に格納されている携帯電話機1301に固有の端末識別子1317と比較し、当該比較結果として一致結果が

得られた場合には、メモリカード1302の端末識別子1317が、携帯電話機1301によってメモリカード1302に書き込まれたものであると判別することができる。

このように、メモリカード1302に格納されている端末識別子1317が、
5 携帯電話機1301によってメモリカード1302に書き込まれたものであることが判ると、暗号化/復号化プログラム1312は、メモリカード1302において端末識別子1317に対応付けられた、通常領域1305の暗号化コンテンツ1307を復号化し、当該復号化されたコンテンツ1315をRAM1314に格納する。

10 図15は、携帯電話機1301のRAM1314に格納されているコンテンツ1315を、メモリカード1302に格納する際の、認証プログラム1309及び暗号化/復号化プログラム1312の処理手順を示すフロー図である。

図15に示すように、認証プログラム1309は、ステップST1401において、まず、メモリカード1302との間で認証を行う。因みに、メモリカード1302には、図示しない認証プログラムが設けられており、携帯電話機
15 1301の認証プログラム1309との間で認証処理を行い、当該認証結果として携帯電話機1301がメモリカード1302の認証領域1303にアクセス可能な端末装置であるという結果が得られると、認証領域1303へのアクセスを許可するようになされている。

20 ステップST1401における認証処理の結果として、携帯電話機1301からメモリカード1302の認証領域1303へのアクセスが可能になると、認証プログラム1309は、当該認証結果を暗号化/復号化プログラム1312に通知する。この通知を受け取った暗号化/復号化プログラム1312は、ステップST1402において、ROM1316から端末識別子1317を取得す
25 る。そして、暗号化/復号化プログラム1312は、ステップST1403に移って、このときメモリカードインターフェイス106に装着されているメモリカード1302の認証領域1303に、ステップST1402においてROM

1 3 1 6 から取得した端末識別子 1 3 1 7 と同じ端末識別子が既に格納されているか否かを判断する。ここで否定結果が得られると、このことは、メモリカード 1 3 0 2 には、携帯電話機 1 3 0 1 によって書き出された端末識別子 1 3 1 7 が格納されていないことを意味しており、このとき暗号化/復号化プログラム 1 3 1 2 は、ステップ S T 1 4 0 4 に移って、ステップ S T 1 4 0 2 において取得した端末識別子 1 3 1 7 とリンク情報 1 3 0 8 を、メモリ書出プログラム 1 0 7 を用いてメモリカード 1 3 0 2 に格納した後、ステップ S T 1 4 0 5 に移る。この場合、暗号化/復号化プログラム 1 3 1 2 は、端末識別子 1 3 1 7 を認証領域 1 3 0 3 に格納するとともに、リンク情報 1 3 0 8 を通常領域 1 3 0 5 のコンテンツ格納ディレクトリ 1 3 0 6 に格納する。リンク情報 1 3 0 8 は、認証領域 1 3 0 3 に格納された端末識別子 1 3 1 7 と、これに対応付けられた、通常領域 1 3 0 5 のコンテンツ格納ディレクトリ 1 3 0 6 に格納される暗号化コンテンツ 1 3 0 7 とを対応付けるための情報である。

また、ステップ S T 1 4 0 3 において肯定結果が得られると、このことは、メモリカード 1 3 0 2 には、携帯電話機 1 3 0 1 によって書き出された端末識別子 1 3 1 7 が格納されていることを意味しており、このとき暗号化/復号化プログラム 1 3 1 2 は、ステップ S T 1 4 0 5 に移る。

ステップ S T 1 4 0 5 において、暗号化/復号化プログラム 1 3 1 2 は、RAM 1 3 1 4 からコンテンツ 1 3 1 5 を取得した後、ステップ S T 1 4 0 6 に移って、ステップ S T 1 4 0 5 において取得したコンテンツ 1 3 1 5 を、ROM 1 3 1 6 内の端末識別子 1 3 1 7 を用いて例えばトリプル DES 暗号方式で暗号化する。

そして、暗号化/復号化プログラム 1 3 1 2 は、ステップ S T 1 4 0 7 に移って、ステップ S T 1 4 0 6 において暗号化された暗号化コンテンツ 1 3 0 7 を、ステップ S T 1 4 0 4 においてメモリカード 1 3 0 2 に格納された端末識別子 1 3 1 7 とリンク情報 1 3 0 8 によって対応付けられたディレクトリに格納する。

- これにより、図16に示すように、メモ리카ード1302においては、それぞれ同じ端末識別子1317によって暗号化されたコンテンツ1315（暗号化コンテンツ1307）と端末識別子1317とが、リンク情報1308によって対応付けられて格納された状態となる。このように、暗号化コンテンツ1307と端末識別子1317とをリンク情報1308によって対応付けるとともに、暗号化コンテンツ1307の存在を確認するための端末識別子1317を認証領域1303に格納することにより、認証領域1303にアクセスが可能な携帯電話機1301のみによって暗号化コンテンツ1307の存在を確認することが可能な状態となる。
- 10 また、図17は、図15の処理手順によってメモ리카ード1302に格納された暗号化コンテンツ1307と端末識別子1317とを携帯電話機1301によって読み込んで復号化する際の、暗号化/復号化プログラム1312とコンテンツ格納ディレクトリ判別プログラム1313との処理手順を示すフロー図である。
- 15 図17に示すように、コンテンツ格納ディレクトリ判別プログラム1313は、ステップST1601において、メモ리카ード1301の通常領域1305にリンク情報1308があるか否かを判断する。ここで否定結果が得られると、このことは、リンク情報1308がメモ리카ード1302に格納されていないこと、すなわち、暗号化コンテンツ1307が格納されていないことを意味しており、このときコンテンツ格納ディレクトリ判別プログラム1313は、
- 20 当該処理手順を終了する。
- これに対して、ステップST1601において肯定結果が得られると、このことは、リンク情報1308がメモ리카ード1302に格納されていること、すなわち、暗号化コンテンツ1307が存在することを意味しており、このとき、コンテンツ格納ディレクトリ判別プログラム1313は、ステップST1602に移って、認証プログラム1309による認証処理を行った上で、メモリ読込プログラム108を用いてメモ리카ード1302から、リンク情報13

08に対応する端末識別子1317を認証領域1303から取得する。

そして、コンテンツ格納ディレクトリ判別プログラム1313は、ステップST1603に移って、ステップST1602において取得した端末識別子と、ROM1316に格納されている端末識別子1317とを比較し、取得した端末識別子と、ROM1316に格納されている端末識別子1317とが同一であるか否かを判断する。

因みに、携帯電話機1301は、コンテンツ1315を暗号化してメモリカード1302に書き出す場合には、常に、端末識別子1317を、暗号化コンテンツ1307に対応付けて格納するようになっている。従って、ステップST1602において取得された端末識別子と、ROM1316に格納されている端末識別子1317との比較結果が一致する場合、このことは、このときメモリカード1302から取得された端末識別子が携帯電話機1301によってメモリカード1302に書き出されたもの、すなわち、当該端末識別子1317とリンク情報1308によって対応付けられてメモリカード1302に格納されている暗号化コンテンツ1307が携帯電話機1301によってメモリカード1302に書き出されたものであることを意味する。

従って、ステップST1602においてメモリカード1302から取得された端末識別子1317と、ROM1316に格納されている端末識別子1317との比較結果が一致する場合、コンテンツ格納ディレクトリ判別プログラム1313は、当該一致結果を暗号化/復号化プログラム1312に通知するとともに、ステップST1603からステップST1604に移る。

これに対して、ステップST1602においてメモリカード1302から取得された端末識別子と、ROM1316に格納されている端末識別子1317との比較結果が一致しない場合、コンテンツ格納ディレクトリ判別プログラム1313は、当該不一致の結果を暗号化/復号化プログラム1312に通知するとともに、上述のステップST1601に戻って、メモリカード1302内に次のリンク情報1308があるか否かを判断し、次のリンク情報1308があ

る場合には、そのリンク情報1308について同様の処理を実行する。

ステップST1604において、コンテンツ格納ディレクトリ判別プログラム1313は、上述のステップST1603において一致結果が得られた端末識別子1317の情報、または、当該端末識別子1317にリンク情報1308によって対応付けられたディレクトリ1306に格納されている暗号化コンテンツ1307に関する情報を液晶画面116に一覧表示する。

これにより、液晶画面116には、メモ리카ード1302に格納されている暗号化コンテンツのうち、携帯電話機1301によって利用可能な暗号化コンテンツ1307に関連する情報が一覧表示される。

- 10 因みに、携帯電話機1301によって利用可能な暗号化コンテンツ1307に関する情報を一覧表示する構成としては、暗号化コンテンツ1307をメモ리카ード1302に格納する際に、その暗号化コンテンツ1307に対応したタイトル等の簡易情報のみを携帯電話機1301のRAM1314に格納し、
- 15 ステップST1603における一致結果に基づいて、当該格納されている簡易情報を一覧表示する等の方法も考えられる。

ステップST1604において、液晶画面116にコンテンツの一覧が表示されると、利用者は、入力インターフェイス117を操作することにより、当該表示された一覧のなかから所望とするコンテンツを選択する。

- これにより、暗号化/復号化プログラム1312は、ステップST1605に移って、メモリ読込プログラム108を用いて、このとき入力インターフェイス117を介して指定された暗号化コンテンツ1307をメモ리카ード1302から読み込み、さらに続くステップST1606に移って、ステップST1605においてメモ리카ード1302から取得した暗号化コンテンツ1307を、ROM1316に格納されている端末識別子1317を用いて復号化
- 25 し、RAM1314に格納する。

RAM1314に格納されたコンテンツ1315は、携帯電話機1301の利用者が入力インターフェイス117を操作することにより起動され、利用者

の利用に供される。

以上の構成において、携帯電話機1301は、メモ리카ード1302に暗号化コンテンツ1307を書き出す際に、当該暗号化コンテンツ1307に対応付けられた端末識別子1317をメモ리카ード1302の認証領域1303
5 に格納しておく。

この端末識別子1317は、例えば、携帯電話機1301の電話番号等であり、暗号化コンテンツ1307に比べてそのデータ量は格段に少ないものとなっている。従って、携帯電話機1301は、メモ리카ード1302から暗号化コンテンツ1307を読み込んで復号化する前に、当該暗号化コンテンツ13
10 07に対応付けられた端末識別子1317をメモ리카ード1302から読み込み、当該端末識別子1317が携帯電話機1301によってメモ리카ード1302に書き出されたものであるか否かを判別することにより、データ量の少ない端末識別子1317に基づいて、携帯電話機1301において利用可能なコンテンツが、メモ리카ード1302に存在するか否かを容易に判断すること
15 ができる。

この実施の形態の場合、端末識別子1317は、認証領域1303に格納されていることにより、携帯電話機1301からメモ리카ード1302の認証領域1303へのアクセスは、認証処理を行った上で実行される。従って、認証領域1303へのアクセスが可能な携帯電話機1301以外の端末装置では、
20 端末識別子1317の取得が困難となることにより、利用可能である暗号化コンテンツの判別を容易に行うことは困難となる。

このように、本実施の形態のコンテンツ処理装置としての携帯電話機1301によれば、コンテンツ蓄積媒体であるメモ리카ード1302に格納された複数の暗号化コンテンツの判別を、認証が可能な携帯電話機1301においての
25 み一段と容易に行うことが可能となる。

なお、この実施の形態においては、携帯電話機1301のROM1316に格納されている端末識別子1317を、暗号化せずにメモ리카ード1302の

認証領域 1 3 0 3 に格納する場合について述べたが、これに限らず、暗号化した後にメモ리카ード 1 3 0 2 の認証領域 1 3 0 3 に格納するようにしてもよい。

また、この実施の形態においては、携帯電話機 1 3 0 1 の ROM 1 3 1 6 に
5 格納されている端末識別子 1 3 1 7 をそのまま、メモ리카ード 1 3 0 2 の認証領域 1 3 0 3 に格納する場合について述べたが、これに限らず、端末識別子 1 3 1 7 を所定の変換式によって変換したものを認証領域 1 3 0 3 に格納するとともに、当該認証領域 1 3 0 3 から当該変換されたものを携帯電話機 1 3 0 1 に読み込んでこれを逆変換式によって逆変換し、ROM 1 3 1 6 の端末識別子 1 3 1 7 と比較するようにしてもよい。この場合、変換式としては、端末識別子 1 3 1 7 の特定の位置（例えば下 4 桁）を抜き出したり、または、端末識別子 1 3 1 7 の文字列を並び替える等、種々の変換式を用いることができる。

なお、この実施の形態の携帯電話機 1 3 0 1 においては、端末識別子 1 3 1 7 として、その携帯電話機 1 3 0 1 の電話番号を用いる場合について述べたが、
15 これに限らず、例えば携帯電話機 1 3 0 1 の製造番号のようなその携帯電話機 1 3 0 1 を識別するための識別子、又は、その他の何らかの意味を持つ文字列、数値、画像または音声等のデータ、若しくは特定のサービスと契約したことを示す識別子（会員番号等）を用いるようにしてもよい。また、この端末識別子 1 3 1 7 として電話番号、製造番号、又はその他の文字列等の情報そのものではなく、端末識別子に対してある変換を加えた結果（端末識別子に関連する情報）を用いるようにしてもよい。このようにすれば、端末識別子によってコンテンツを暗号化する際の暗号化方法、及び端末識別子が第三者に漏洩した場合であっても、その端末識別子は、暗号化鍵となり得る他のデータに変換されていることにより、このデータ（暗号化鍵）によって暗号化された暗号化コンテンツが
20 25 解読されることを防止することができる。

また、この実施の形態においては、コンテンツ 1 3 1 5 を端末識別子 1 3 1 7 を用いて暗号化し、メモ리카ード 1 3 0 2 に格納する場合について述べたが、

これに限らず、コンテンツ 1315 を端末識別子 1317 に関連する情報を用いて暗号化するようにしてもよい。

- また、この実施の形態においては、通常領域に格納されたリンク情報によって認証領域の端末識別子を特定する場合について述べたが、これに限らず、例えば、通常領域に格納されている暗号化コンテンツの当該通常領域での格納位置を示す情報（ルート名、ディレクトリ名等）と、これに対応して認証領域に格納されている端末識別子の当該認証領域での格納位置を示す情報（ルート名、ディレクトリ名等）を同一とするようにしてもよい。このように同じディレクトリ構成とすれば、リンク情報を用いることなく認証領域での端末識別子と通常領域の暗号化コンテンツとを対応付けることができる。

また、この実施の形態においては、コンテンツを格納するコンテンツ蓄積媒体としてメモリカード 1302 を用いる場合について述べたが、これに限らず、要はデジタル情報化されたコンテンツを格納可能なコンテンツ蓄積媒体であれば、他のデバイスを広く適用することができる。

15 （実施の形態 5）

図 18 は、本発明の実施の形態 5 に係るコンテンツ処理装置としての携帯電話機 1701 の構成を示すブロック図である。但し、図 1 及び図 2 と同一の構成となるものについては、図 1 及び図 2 と同一番号を付し、詳しい説明を省略する。

- この図 18 に示される携帯電話機 1701 は、ROM 1713 に格納される端末識別子として、コンテンツ 1712 を暗号化するための暗号化用端末識別子 1714 と、メモリカード 1702 内の暗号化コンテンツを格納するコンテンツ格納ディレクトリ（以下、これを単にディレクトリと称する）1703 のディレクトリ名 1704 として用いるディレクトリ判別用端末識別子 1715 とを用意した点が図 2 の構成の携帯電話機 101 と異なる。

図 2 との対応部分に同一符号を付して示す図 18 は、携帯電話機 1701 の構成を示すブロック図である。この図 18 は、携帯電話機 1701 の構成のう

ち、特にコンテンツ処理に関わる構成を抽出して示すものである。携帯電話機 1701 は、それぞれ図示しない CPU (Central Processing Unit) によって動作するメモリ書出プログラム 107、メモリ読込プログラム 108、暗号化/復号化プログラム 1709 及びコンテンツ格納ディレクトリ判別プログラム 1710 を含んでいる。

図 18 において、携帯電話機 1701 は、コンテンツプロバイダから携帯電話回線網を介してダウンロードしたコンテンツ 1712 を RAM (Random Access Memory) 1711 に格納する。暗号化/復号化プログラム 1709 は、RAM 1711 に格納されたコンテンツ 1712 を暗号化するものであり、当該暗号化/復号化プログラム 1709 によって暗号化されたコンテンツ 1712 は、暗号化コンテンツ 1705 として、メモリ書出プログラム 107 によってメモリカードインターフェイス 106 を介してメモリカード 1702 に書き込まれる。

ROM (Read Only Memory) 1713 は、携帯電話機 1701 に固有の所定の文字列 (製造番号等) でなる識別子であって、コンテンツ 1712 を暗号化する際に用いられる暗号化用端末識別子 1714 と、携帯電話機 1701 に固有の所定の文字列 (電話番号等) でなる識別子であって、暗号化コンテンツをメモリカード 1702 に格納する際に用いられるディレクトリ名 1704 となるディレクトリ判別用端末識別子 1715 を格納している。暗号化用端末識別子 1714 とディレクトリ判別用端末識別子 1715 とは、互いに異なる文字列が用いられる。

暗号化/復号化プログラム 1709 は、コンテンツ 1712 を暗号化する際、ROM (Read Only Memory) 1713 に格納されている暗号化用端末識別子 1714 を用いて暗号化する。また、暗号化/復号化プログラム 1709 は、当該暗号化されたコンテンツ 1712 (暗号化コンテンツ 1705) をメモリカード 1702 に格納する際、当該格納先となるディレクトリ 1703 のディレクトリ名 1704 を、ROM 1713 に格納されているディレクトリ判別用端

末識別子1715の端末識別子名とする。

また、メモ리카ード1702に格納された暗号化コンテンツ1705を携帯電話機1701に読み込む場合、携帯電話機1701のメモリ読込プログラム108は、暗号化コンテンツ1705を読み込む処理に先立って、当該暗号化
5 コンテンツ1705が格納されているディレクトリ名1704をメモ리카ード1702から取得し、当該取得されたディレクトリ名1704とROM1713に格納されているディレクトリ判別用端末識別子1715とが一致した場合には、当該取得したメモ리카ード1702のディレクトリ名1704が、携帯電話機1701によってメモ리카ード1702に設定されたものである
10 と判別することができる。

このように、メモ리카ード1702に設定されているディレクトリ名1704が、携帯電話機1701によってメモ리카ード1702に設定されたものであることが判ると、暗号化/復号化プログラム1709は、当該ディレクトリ名1704によって表わされるディレクトリ1703に格納されている暗号化
15 コンテンツ1705を復号化し、当該復号化されたコンテンツ1712をRAM1711に格納する。

図19は、携帯電話機1701のRAM1711に格納されているコンテンツ1712を、メモ리카ード1702に格納する際の、暗号化/復号化プログラム1709の処理手順を示すフロー図である。

20 図19に示すように、暗号化/復号化プログラム1709は、ステップST1801において、ROM1713からディレクトリ判別用端末識別子1715を取得する。そして、暗号化/復号化プログラム1709は、ステップST1802に移って、ステップST1801において取得したディレクトリ判別用端末識別子1715の識別子名と同じディレクトリ名1704のディレクトリ
25 1703がメモ리카ード1702にあるか否かを判断する。

ここで否定結果が得られると、このことは、メモ리카ード1702には、携帯電話機1701によって設定されたディレクトリ1703が存在しないこ

とを意味しており、このとき、暗号化/復号化プログラム1709は、ステップST1803に移って、ROM1713に格納されているディレクトリ判別用端末識別子1715の識別子名と同じディレクトリ名1704のディレクトリ1703を作成し、ステップST1804に移る。

- 5 これに対して、ステップST1802において肯定結果が得られると、このことは、既に携帯電話機1701によって作成されたディレクトリ1703がメモ리카ード1702に存在することを意味しており、このとき暗号化/復号化プログラム1709はステップST1804に移る。

- 10 ステップST1804において、暗号化/復号化プログラム1709は、RAM1711からコンテンツ1712を取得した後、ステップST1805に移って、ステップST1804において取得したコンテンツ1712を、ROM1713内の暗号化端末識別子1714を用いて例えばトリプルDES暗号方式で暗号化する。

- 15 そして、暗号化/復号化プログラム1709は、ステップST1806に移って、ステップST1805において暗号化された暗号化コンテンツ1705を、ステップST1803において作成されたディレクトリ名1704のディレクトリ1703に格納する。

- 20 これにより、図20に示すように、メモ리카ード1702においては、それぞれ同じ暗号化用端末識別子1714によって暗号化されたコンテンツ1712（暗号化コンテンツ1705）、すなわち一つの携帯電話機1701によって書き出された暗号化コンテンツ1705が、当該携帯電話機固有の端末識別子名と同じディレクトリ名1704のディレクトリ1703に格納された状態となる。

- 25 また、図21は、図19の処理手順によってメモ리카ード1702に格納された暗号化コンテンツ1705を携帯電話機1701によって読み込んで復号化する際の、暗号化/復号化プログラム1709とコンテンツ格納ディレクトリ判別プログラム1710との処理手順を示すフロー図である。

図21に示すように、コンテンツ格納ディレクトリ判別プログラム1710は、ステップST2001において、メモリカード1702内にディレクトリがあるか否かを調べる。ここで否定結果が得られると、このことは、メモリカード1702には、読み込むべき暗号化コンテンツ1705がないことを意味
5 しており、このときコンテンツ格納ディレクトリ判別プログラム1710は、この処理手順を終了する。

これに対して、ステップST2001において肯定結果が得られると、このことは、メモリカード1702には、読み込むべき暗号化コンテンツ1705があることを意味しており、このときコンテンツ格納ディレクトリ判別プログラム1710は、ステップST2002に移って、メモリ読込プログラム10
8を用いてメモリカード1702からディレクトリ名を取得した後、ステップST2003に移る。ステップST2003において、コンテンツ格納ディレクトリ判別プログラム1710は、ステップST2002において取得したディレクトリ名が、ROM1713に格納されているディレクトリ判別用端末識
15 別子1715と同一であるか否かを判断する。

ここで否定結果が得られると、このことは、このときメモリカード1702から取得したディレクトリ名が、携帯電話機1701によって設定されたディレクトリ名1704ではないこと、すなわち、そのディレクトリに格納されている暗号化コンテンツは、携帯電話機1701によって利用できないものであ
20 ることを意味しており、このとき、コンテンツ格納ディレクトリ判別プログラム1710は、当該不一致の結果を暗号化/復号化プログラム1709に通知するとともに、上述のステップST2001に戻って、メモリカード1702内に次のディレクトリがあるか否かを判断し、次のディレクトリがある場合には、そのディレクトリについて同様の処理を実行する。

25 これに対して、ステップST2003において肯定結果が得られると、このことは、このとき取得したディレクトリ名が、携帯電話機1701によって設定されたもの、すなわち、そのディレクトリ1703に格納されている暗号化

コンテンツ１７０５は、携帯電話機１７０１によって利用できるものであることを意味しており、このとき、コンテンツ格納ディレクトリ判別プログラム１７１０は、当該一致の結果を暗号化/復号化プログラム１７０９に通知するとともに、ステップＳＴ２００４に移る。

- ５ ステップＳＴ２００４において、コンテンツ格納ディレクトリ判別プログラム１７１０は、上述のステップＳＴ２００３において一致結果が得られたディレクトリ名１７０４に関する情報、または、当該ディレクトリ名１７０４のディレクトリ１７０３に格納されている暗号化コンテンツ１７０５に関連する情報を液晶画面１１６に一覧表示する。

- 10 これにより、液晶画面１１６には、メモリカード１７０２に格納されている暗号化コンテンツのうち、携帯電話機１７０１によって利用可能な暗号化コンテンツ１７０５に関連する情報が一覧表示される。

- 因みに、携帯電話機１７０１によって利用可能な暗号化コンテンツ１７０５に関する情報を一覧表示する構成としては、暗号化コンテンツ１７０５をメモリカード１７０２に格納する際に、その暗号化コンテンツ１７０５に対応した
15 タイトル等の簡易情報のみを携帯電話機１７０１のＲＡＭ１７１１に格納し、ステップＳＴ２００３における一致結果に基づいて、当該格納されている簡易情報を一覧表示する等の方法も考えられる。

- ステップＳＴ２００４において、液晶画面１１６にコンテンツの一覧が表示
20 されると、利用者は、入力インターフェイス１１７を操作することにより、当該表示された一覧のなかから所望とするコンテンツを選択する。

- これにより、暗号化/復号化プログラム１７０９は、ステップＳＴ２００５に移って、メモリ読込プログラム１０８を用いて、このとき入力インターフェイス１１７を介して指定された暗号化コンテンツ１７０５をメモリカード１７
25 ０２から読み込み、さらに続くステップＳＴ２００６に移って、ステップＳＴ２００５においてメモリカード１７０２から取得した暗号化コンテンツ１７０５を、ＲＯＭ１７１３に格納されている暗号化用端末識別子１７１４を用い

て復号化し、RAM 1711に格納する。

RAM 1711に格納されたコンテンツ 1712は、携帯電話機 1701の利用者が入力インターフェイス 117を操作することにより起動され、利用者の利用に供される。

- 5 以上の構成において、携帯電話機 1701は、メモリカード 1702に暗号化コンテンツ 1705を書き出す際に、当該暗号化コンテンツ 1705を格納するディレクトリのディレクトリ名 1704として、当該携帯電話機 1701に固有のディレクトリ判別用端末識別子 1715を用いる。

- このディレクトリ名は、暗号化コンテンツ 1705に比べてそのデータ量は
10 格段に少ないものとなっている。従って、携帯電話機 1701は、メモリカード 1702から暗号化コンテンツ 1705を読み込んで復号化する前に、当該暗号化コンテンツ 1705が格納されたディレクトリのディレクトリ名 1704を読み込んで、当該ディレクトリ名が携帯電話機 1701のディレクトリ判別用端末識別子 1715と一致するか否かを判別する。

- 15 ディレクトリ名が携帯電話機 1701のディレクトリ判別用端末識別子 1715と一致する場合、当該ディレクトリ名 1704が付けられたディレクトリに格納されている暗号化コンテンツ 1705は、携帯電話機 1701によってメモリカード 1702に書き出されたものであることになる。

- 従って、この暗号化コンテンツ 1705は、携帯電話機 1701に読み込んで、当該携帯電話機 1701によって利用することが可能であり、携帯電話機
20 1701の暗号化/復号化プログラム 1709は、メモリカード 1702から暗号化コンテンツ 1705を読み込み、当該読み込まれた暗号化コンテンツ 1705を復号化する。

- このように、ディレクトリ名が、ROM 1713に格納されているディレ
25 クトリ判別用端末識別子 1715と一致することを条件に、当該ディレクトリ名 1704が付けられたディレクトリに格納されている暗号化コンテンツ 1705をメモリカード 1702から携帯電話機 1701に読み込んで復号化す

ることにより、携帯電話機1701は、当該携帯電話機1701において利用可能である暗号化コンテンツ1705のみを、データ量の少ないディレクトリ名に基づいて選択することができる。

- 従って、メモリカード1702に複数の暗号化コンテンツが格納されている
- 5 状態であって、これら複数の暗号化コンテンツを利用可能な端末装置（携帯電話機等）が各暗号化コンテンツ毎に異なる場合であっても、携帯電話機1701は、これら複数のデータ量の多い暗号化コンテンツをすべて復号化する必要はなく、当該複数の暗号化コンテンツにそれぞれ対応付けられた、データ量の少ないディレクトリを取得するだけで、利用可能な暗号化コンテンツ1705
- 10 を判別することができる。

- また、ディレクトリ名1704として用いられるコンテンツ判別用端末識別子1714とは異なる暗号化用端末識別子1714によってコンテンツ1712を暗号化し、これをコンテンツ判別用端末識別子1714と同じディレクトリ名1704が付けられたディレクトリに格納することにより、ディレクトリ名1704が第三者に知られた場合であっても、暗号化コンテンツ1705
- 15 が不正に復号化されることを防止することができる。

- このように、本実施の形態のコンテンツ処理装置としての携帯電話機1701によれば、コンテンツ蓄積媒体であるメモリカード1702に格納された複数の暗号化コンテンツの判別を一段と容易に行うことが可能となり、携帯電話
- 20 機1701において利用可能な暗号化コンテンツ1705を一段と迅速に復号化することができる。

- なお、この実施の形態においては、携帯電話機1701のROM1713に格納されているディレクトリ判別用端末識別子1715を暗号化せずに、メモリカード1702の暗号化コンテンツ格納用のディレクトリ名1704とした場合について述べたが、これに限らず、ディレクトリ判別用端末識別子1715を暗号化してディレクトリ名としてもよい。
- 25

また、この実施の形態においては、暗号化コンテンツ1705を格納するメ

メモリカード1702のディレクトリ1704として、ディレクトリ判別用端末識別子1715を用いる場合について述べたが、これに限らず、図2について上述した特定データ115を用いるようにしてもよい。

また、この実施の形態の携帯電話機1701においては、暗号化用端末識別子1714及びディレクトリ判別用端末識別子1715として、電話番号、製造番号等を用いる場合について述べたが、これに限らず、何らかの意味を持つ文字列、数値、画像または音声等のデータ、若しくは特定のサービスと契約したことを示す識別子（会員番号等）を用いるようにしてもよい。また、この暗号化用端末識別子1714及びディレクトリ判別用端末識別子1715として電話番号、製造番号、又はその他の文字列等の情報そのものではなく、これらの端末識別子（暗号化用端末識別子1714及びディレクトリ判別用端末識別子1715）に対してそれぞれある変換を加えた結果（端末識別子に関連する情報）をそれぞれ用いるようにしてもよい。このようにすれば、端末識別子によってコンテンツを暗号化する際の暗号化方法、及び端末識別子が第三者に漏洩した場合であっても、その端末識別子は、暗号化鍵となり得る他のデータに変換されていることにより、このデータ（暗号化鍵）によって暗号化された暗号化コンテンツが解読されることを防止することができる。

また、この実施の形態においては、コンテンツ1712を暗号化用端末識別子1714を用いて暗号化し、メモリカード1702に格納する場合について述べたが、これに限らず、コンテンツ1712を暗号化用端末識別子1714に関連する情報を用いて暗号化するようにしてもよい。

また、この実施の形態においては、コンテンツを格納するコンテンツ蓄積媒体としてメモリカード1702を用いる場合について述べたが、これに限らず、要はデジタル情報化されたコンテンツを格納可能なコンテンツ蓄積媒体であれば、他のデバイスを広く適用することができる。

（実施の形態6）

図22は、本発明の実施の形態6に係るコンテンツ処理装置としての携帯電

話機 2101 の構成を示すブロック図である。但し、図 1 及び図 2 と同一の構成となるものについては、図 1 及び図 2 と同一番号を付し、詳しい説明を省略する。

この図 22 に示される携帯電話機 2101 は、RAM 2111 に格納されて
5 いるコンテンツ 2112 をメモリカード 2102 に書き出す際に、図 2 について上述した特定データ 115 に代えて、その書出し時刻を暗号化コンテンツ 2105 に対応付けて書き出す点が図 2 の構成の携帯電話機 101 と異なる。

図 2 との対応部分に同一符号を付して示す図 22 は、携帯電話機 2101 の構成を示すブロック図である。この図 22 は、携帯電話機 2101 の構成のうち、特にコンテンツ処理に関わる構成を抽出して示すものである。携帯電話機
10 2101 は、それぞれ図示しない CPU (Central Processing Unit) によって動作するメモリ書出プログラム 107、メモリ読込プログラム 108、暗号化/復号化プログラム 2109、コンテンツ格納ディレクトリ判別プログラム 2110 及び時刻特定プログラム 2119 を含んでいる。

図 22 において、携帯電話機 2101 は、コンテンツプロバイダから携帯電話回線網を介してダウンロードしたコンテンツ 2112 を RAM (Random Access Memory) 2111 に格納する。暗号化/復号化プログラム 2109 は、RAM 2111 に格納されたコンテンツ 2112 を暗号化するものであり、当該暗号化/復号化プログラム 2109 によって暗号化されたコンテンツ 211
20 2 は、暗号化コンテンツ 2105 として、メモリ書出プログラム 107 によってメモリカードインターフェイス 106 を介してメモリカード 2102 に書き込まれる。

ROM (Read Only Memory) 2114 は、携帯電話機 2101 に固有の所定の文字列 (電話番号等) でなる識別子であって、コンテンツ 2112 を暗号
25 化する際に用いられる端末識別子 2115 を格納している。

暗号化/復号化プログラム 2109 は、コンテンツ 2112 を暗号化する際、ROM (Read Only Memory) 2113 に格納されている端末識別子 2115

を用いて暗号化する。また、暗号化/復号化プログラム2109は、当該暗号化されたコンテンツ2112（暗号化コンテンツ2105）をメモ리카ード2102に格納する際、時刻特定プログラム2119によって特定される書出時刻を表わす書出時刻情報2113を、メモ리카ード2102の暗号化コンテンツ2105が格納されたディレクトリと同じディレクトリに格納する。これにより、暗号化コンテンツ2105とその書出時刻情報2113とが対応付けられてメモ리카ード2102に格納された状態となる。また、メモ리카ード2102に格納された書出時刻情報2113は、暗号化/復号化プログラム2109及び時刻特定プログラム2119によって携帯電話機2101のRAM2111にも格納される。

また、メモ리카ード2102の所定のディレクトリ2103に格納された暗号化コンテンツ2105を携帯電話機2101に読み込む場合、携帯電話機2101のメモリ読込プログラム108は、暗号化コンテンツ2105を読み込む処理に先立って、携帯電話機2101のRAM2111に格納されている書出時刻情報2113と一致する書出時刻情報2113に対応付けられてメモ리카ード2102に格納されている暗号化コンテンツ2105を一覧情報化する。この一覧に載せられた暗号化コンテンツ2105は、携帯電話機2101によってメモ리카ード2102に書き出されたものであると判別することができる。

このように、メモ리카ード2102に格納されている書出時刻情報2113が、携帯電話機2101によってメモ리카ード2102に格納されたものであることが判ると、暗号化/復号化プログラム2109は、当該書出時刻情報2113に対応付けられて格納されている暗号化コンテンツ2105を復号化し、当該復号化されたコンテンツ2112をRAM2111に格納する。

図23は、携帯電話機2101のRAM2111に格納されているコンテンツ2112を、メモ리카ード2102に格納する際の、暗号化/復号化プログラム2109及び時刻特定プログラム2119の処理手順を示すフロー図であ

る。

図23に示すように、暗号化/復号化プログラム2109は、ステップST2201において、まず、コンテンツ格納用のディレクトリ2103を作成した後、続くステップST2202に移って、RAM2111からコンテンツ2112を取得する。そして、暗号化/復号化プログラム2109は、ステップST2203に移って、ステップST2202において取得したコンテンツ2112を、ROM2114内の端末識別子2115を用いて例えばトリプルDES暗号方式で暗号化する。

そして、暗号化/復号化プログラム2109は、ステップST2204に移って、このときの時刻情報を時刻特定プログラム2119によって生成し、これを書出時刻情報2113としてRAM2111に格納する。これにより、RAM2111には、暗号化コンテンツ2105をメモ리카ード2102に書き出す際、この時刻情報2113が格納される。

そして、暗号化/復号化プログラム2109は、ステップST2205に移って、ステップST2203において暗号化された暗号化コンテンツ2105を、ステップST2204において生成された書出時刻情報2113とともに、ステップST2201において作成されたメモ리카ード2102のディレクトリ2103に格納する。

これにより、図24に示すように、メモ리카ード2102においては、暗号化コンテンツ2105が、メモ리카ード2102へのその書出時刻を表わす書出時刻情報2113とともに同じディレクトリ2103に対応付けられて格納された状態となる。

また、図25は、図23の処理手順によってメモ리카ード2102に格納された暗号化コンテンツ2105を携帯電話機2101によって読み込んで復号化する際の、暗号化/復号化プログラム2109とコンテンツ格納ディレクトリ判別プログラム2110との処理手順を示すフロー図である。

図25に示すように、コンテンツ格納ディレクトリ判別プログラム2110

は、ステップST2401において、メモリカード2102内に暗号化コンテンツがあるか否かを調べる。ここで肯定結果が得られると、このことは、携帯電話機2101によってメモリカード2102に書き出された暗号化コンテンツ、すなわち携帯電話機2101によって利用可能な暗号化コンテンツ2105がメモリカード2102に格納されている可能性があることを意味しており、このとき、コンテンツ格納ディレクトリ判別プログラム2110は、ステップST2402に移って、暗号化コンテンツと同一ディレクトリにある書出時刻情報を取得する。

そして、コンテンツ格納ディレクトリ判別プログラム2110は、ステップST2403に移って、ステップST2402において取得した書出時刻情報が、携帯電話機2101のRAM2111に格納されている書出時刻情報2113と同一であるか否かを判断する。

ここで否定結果が得られると、このことは、このとき取得した書出時刻情報が、携帯電話機2101によってメモリカード2101に書き出されたものではないこと、すなわち、この書出時刻情報と同一のディレクトリに格納されている暗号化コンテンツが、携帯電話機2101によってメモリカード2102に書き出されたものではないことを意味しており、このとき、コンテンツ格納ディレクトリ判別プログラム2110は、上述のステップST2401に戻って、メモリカード2102に他の暗号化コンテンツが格納されているか否かを判断し、当該判断結果に基づいて上述の場合と同様の処理を行う。

これに対して、ステップST2403において肯定結果が得られると、このことは、このとき取得した書出時刻情報が、携帯電話機2101によってメモリカード2101に書き出された書出時刻情報2113であること、すなわち、この書出時刻情報2113と同一のディレクトリ2103に格納されている暗号化コンテンツ2105が、携帯電話機2101によってメモリカード2102に書き出されたものであることを意味しており、このとき、コンテンツ格納ディレクトリ判別プログラム2110は、ステップST2404に移って、

当該書出時刻情報 2 1 1 3 を一覧情報に追加した後、上述のステップ S T 2 4 0 1 に戻って、メモリカード 2 1 0 2 に他の暗号化コンテンツが格納されているか否かを判断し、当該判断結果に基づいて上述の場合と同様の処理を行う。

そして、メモリカード 2 1 0 2 に格納されている暗号化コンテンツ（書出時刻情報）のすべてについて、携帯電話機 2 1 0 1 によって書き出されたものであるか否かの判断が完了すると、コンテンツ格納ディレクトリ判別プログラム 2 1 1 0 は、ステップ S T 2 4 0 1 において否定結果を得ることにより、ステップ S T 2 4 0 5 に移って、上述のステップ S T 2 4 0 4 において作成された一覧情報によって特定される暗号化コンテンツ 2 1 0 5 に関する情報を液晶画面 1 1 6 に一覧表示する。

これにより、液晶画面 1 1 6 には、メモリカード 2 1 0 2 に格納されている暗号化コンテンツのうち、携帯電話機 2 1 0 1 によって利用可能な暗号化コンテンツ 2 1 0 5 に関連する情報（書出時刻情報等）が一覧表示される。

因みに、携帯電話機 2 1 0 1 によって利用可能な暗号化コンテンツ 2 1 0 5 に関する情報を一覧表示する構成としては、暗号化コンテンツ 2 1 0 5 をメモリカード 2 1 0 2 に格納する際に、その暗号化コンテンツ 2 1 0 5 に対応したタイトル等の簡易情報のみを携帯電話機 2 1 0 1 の RAM 2 1 1 1 に格納し、ステップ S T 2 4 0 3 における一致結果に基づいて、当該格納されている簡易情報を一覧表示する等の方法も考えられる。

ステップ S T 2 4 0 5 において、液晶画面 1 1 6 にコンテンツの一覧が表示されると、利用者は、入力インターフェイス 1 1 7 を操作することにより、当該表示された一覧のなかから所望とするコンテンツを選択する。

これにより、暗号化/復号化プログラム 2 1 0 9 は、ステップ S T 2 4 0 6 に移って、メモリ読込プログラム 1 0 8 を用いて、このとき入力インターフェイス 1 1 7 を介して指定された暗号化コンテンツ 2 1 0 5 をメモリカード 2 1 0 2 から読み込み、さらに続くステップ S T 2 4 0 7 に移って、ステップ S T 2 4 0 6 においてメモリカード 2 1 0 2 から取得した暗号化コンテンツ 2 1

05を、ROM2114に格納されている端末識別子2115を用いて復号化し、RAM2111に格納する。

RAM2111に格納されたコンテンツ2112は、携帯電話機2101の利用者が入力インターフェイス117を操作することにより起動され、利用者
5 の利用に供される。

以上の構成において、携帯電話機2101は、メモ리카ード2102に暗号化コンテンツ2105を書き出す際に、その書出し時刻を時刻特定プログラム2119によってRAM2111に格納する。これにより、携帯電話機2101においては、当該携帯電話機2101においてのみ使用可能な暗号化コンテンツ2105を識別するための情報である書出時刻情報2113が、自身の環境に設定された状態となる。

そして、この設定された書出時刻情報2111は、暗号化コンテンツ2105とともにメモ리카ード2102の同じディレクトリ2103に格納される。これにより、暗号化コンテンツ2105と当該暗号化コンテンツ2105の利
15 用環境（利用可能な携帯電話機2101）を識別するための書出時刻情報2113とが対応付けられてメモ리카ード2102に格納された状態となる。

このように、暗号化コンテンツ2105をメモ리카ード2102に書き出す際
の書出時刻情報2113は、携帯電話機2101が暗号化コンテンツ2105をメモ리카ード2102に書き出したことの事実を表わすキーワードとし
20 て携帯電話機2101及びメモ리카ード2102の双方に格納される。

従って、携帯電話機2101に装着されたメモ리카ード2102に、当該携帯電話機2101に格納されている書出時刻情報2113と同一の時刻情報が格納されている場合には、当該書出時刻情報2113に対応付けられてメモ
リカード2102に格納されている暗号化コンテンツ2105は、携帯電話機
25 2101によって書き出されたもの、すなわち、携帯電話機2101によって利用が可能なコンテンツであることを意味する。

従って、メモ리카ード2102に暗号化コンテンツ2105に対応付けられ

た格納されている書出時刻情報 2 1 1 3 と、携帯電話機 2 1 0 1 に格納されている書出時刻情報 2 1 1 3 とが一致した場合、この書出時刻情報 2 1 1 3 に対応付けられてメモリカード 2 1 0 2 に格納されている暗号化コンテンツ 2 1 0 5 は、携帯電話機 2 1 0 1 に読み込んで、当該携帯電話機 2 1 0 1 によって
5 利用することが可能であり、この一致結果を受けて、携帯電話機 2 1 0 1 の暗号化/復号化プログラム 2 1 0 9 は、メモリカード 2 1 0 2 から暗号化コンテンツ 2 1 0 5 を読み込み、当該読み込まれた暗号化コンテンツ 2 1 0 5 を復号化する。

このように、メモリカード 2 1 0 2 の書出時刻情報 2 1 1 3 が、RAM 2 1
10 1 1 に格納されている書出時刻情報 2 1 1 3 と一致することを条件に、当該書出時刻情報 2 1 1 3 に対応付けられた暗号化コンテンツ 2 1 0 5 をメモリカード 2 1 0 2 から携帯電話機 2 1 0 1 に読み込んで復号化することにより、携帯電話機 2 1 0 1 は、当該携帯電話機 2 1 0 1 において利用可能である暗号化コンテンツ 2 1 0 5 のみを、データ量の少ない書出時刻情報 2 1 1 3 に基づいて選択することができる。
15

従って、メモリカード 2 1 0 2 に複数の暗号化コンテンツが格納されている状態であって、これら複数の暗号化コンテンツを利用可能な端末装置（携帯電話機等）が各暗号化コンテンツ毎に異なる場合であっても、携帯電話機 2 1 0 1 は、これら複数のデータ量の多い暗号化コンテンツをすべて復号化する必要
20 はなく、当該複数の暗号化コンテンツにそれぞれ対応付けられた、データ量の少ない書出時刻情報 2 1 1 3 を取得するだけで、利用可能な暗号化コンテンツ 2 1 0 5 を判別することができる。

このように、本実施の形態のコンテンツ処理装置としての携帯電話機 2 1 0 1 によれば、コンテンツ蓄積媒体であるメモリカード 2 1 0 2 に格納された複数の暗号化コンテンツの判別を一段と容易に行うことが可能となり、携帯電話
25 機 2 1 0 1 において利用可能な暗号化コンテンツ 2 1 0 5 を一段と迅速に復号化することができる。

なお、この実施の形態においては、暗号化コンテンツ 2105 を判別するための情報として、当該暗号化コンテンツ 2105 をメモ리카ード 2102 に書き出した書出時刻情報 2113 を用いる場合について述べたが、これに限らず、利用者が自ら入力インターフェイス 117 を操作して入力した設定情報、または携帯電話機 2101 が乱数等を用いてランダムに設定した値等を用いるようにしてもよい。また、これらの情報は、上述の書出時刻情報 2113 の場合を含めて、暗号化してメモ리카ード 2102 に格納するようにしてもよい。このようにすれば、書出時刻情報 2113 または、その他の暗号化コンテンツ 2105 を判別するための情報（利用者が設定した設定情報、携帯電話機 2101 がランダムに設定した値）が、メモ리카ード 2102 から第三者に知られた場合であっても、暗号化コンテンツ 2105 が不正に復号化されることを防止することができる。また、さらに書出時刻情報 2113 を予め設定されている識別子、または利用者が設定した識別子を用いて暗号化した後にメモ리카ード 2102 に格納するようにしてもよい。

また、この実施の形態においては、書出時刻情報 2113 をそのまま、メモ리카ード 2102 に格納する場合について述べたが、これに限らず、書出時刻情報 2113 を所定の変換式によって変換したものを格納するとともに、当該格納されたものを携帯電話機 2101 に読み込んでこれを逆変換式によって逆変換し、RAM 2111 の書出時刻情報 2113 と比較するようにしてもよい。この場合、変換式としては、書出時刻情報 2113 の特定の位置（例えば下 4 桁）を抜き出したり、または、書出時刻情報 2113 の文字列を並び替える等、種々の変換式を用いることができる。

また、この実施の形態においては、書出時刻情報 2113 を暗号化コンテンツ 2105 と同じディレクトリ 2103 に格納する場合について述べたが、これに限らず、携帯電話機 2101 との間で認証を行うことによりアクセスが可能となる認証領域をメモ리카ード 2102 に設け、書出時刻情報 2113 を当該認証領域に格納するとともに、当該認証領域の書出時刻情報 2113 と通常

領域の暗号化コンテンツ 2105 との関係を表わすリンク情報を暗号化コンテンツ 2105 と同じディレクトリに格納するようにしてもよい。このようにすれば、メモ리카ード 2102 との間で認証に成功した携帯電話機 2101 のみが書出時刻情報 2113 を取得することができる。

- 5 また、この実施の形態の携帯電話機 2101 においては、端末識別子 2115 として、その携帯電話機 2101 の電話番号を用いる場合について述べたが、これに限らず、例えば携帯電話機 2101 の製造番号のようなその携帯電話機 2101 を識別するための識別子、又は、その他の何らかの意味を持つ文字列、数値、画像または音声等のデータ、若しくは特定のサービスと契約したことを示す識別子（会員番号等）を用いるようにしてもよい。また、この端末識別子
- 10 2115 として電話番号、製造番号、又はその他の文字列等の情報そのものではなく、端末識別子に対してある変換を加えた結果（端末識別子に関連する情報）を用いるようにしてもよい。このようにすれば、端末識別子によってコンテンツ及び特定データを暗号化する際の暗号化方法、及び端末識別子が第三者
- 15 に漏洩した場合であっても、その端末識別子は、暗号化鍵となり得る他のデータに変換されていることにより、このデータ（暗号化鍵）によって暗号化された暗号化コンテンツ及び暗号化特定データが解読されることを防止することができる。

- また、この実施の形態においては、コンテンツを格納するコンテンツ蓄積媒体としてメモ리카ード 2102 を用いる場合について述べたが、これに限らず、要はデジタル情報化されたコンテンツを格納可能なコンテンツ蓄積媒体であれば、他のデバイスを広く適用することができる。
- 20

（実施の形態 7）

- 図 26 は、本発明の実施の形態 7 に係るコンテンツ処理装置としての携帯電話機 2501 の構成を示すブロック図である。但し、図 1 及び図 2 と同一の構成となるものについては、図 1 及び図 2 と同一番号を付し、詳しい説明を省略する。
- 25

この図26に示される携帯電話機2501は、RAM2511に格納されているコンテンツ2512をメモ리카ード2502に書き出す際に、図2について上述した特定データ115に代えて、そのメモ리카ード2502におけるディレクトリ名2513を暗号化コンテンツ2505に対応付けて設定する点
5 が図2の構成の携帯電話機101と異なる。

図2との対応部分に同一符号を付して示す図26は、携帯電話機2501の構成を示すブロック図である。この図26は、携帯電話機2501の構成のうち、特にコンテンツ処理に関わる構成を抽出して示すものである。携帯電話機2501は、それぞれ図示しないCPU (Central Processing Unit) によって
10 動作するメモリ書出プログラム107、メモリ読込プログラム108、暗号化/復号化プログラム2509及びコンテンツ格納ディレクトリ判別プログラム2510を含んでいる。

図26において、携帯電話機2501は、コンテンツプロバイダから携帯電話回線網を介してダウンロードしたコンテンツ2512をRAM (Random
15 Access Memory) 2511に格納する。暗号化/復号化プログラム2509は、RAM2511に格納されたコンテンツ2512を暗号化するものであり、当該暗号化/復号化プログラム2509によって暗号化されたコンテンツ2512は、暗号化コンテンツ2505として、メモリ書出プログラム107によってメモ리카ードインターフェイス106を介してメモ리카ード2502に書
20 き込まれる。

ROM (Read Only Memory) 2514は、携帯電話機2501に固有の所定の文字列 (電話番号等) でなる識別子であって、コンテンツ2512を暗号化
化する際に用いられる端末識別子2515を格納している。

【0405】

25 暗号化/復号化プログラム2509は、コンテンツ2512を暗号化する際、ROM (Read Only Memory) 2514に格納されている端末識別子2515を用いて暗号化する。また、暗号化/復号化プログラム2509は、当該暗号化

されたコンテンツ 2512（暗号化コンテンツ 2505）をメモリカード 2502 に格納する際、当該格納先であるディレクトリ 2503 を作成し、当該ディレクトリ 2503 に暗号化コンテンツ 2505 を格納する。この携帯電話機 2501 によって作成されたディレクトリ 2503 のディレクトリ名 2513 は、当該携帯電話機 2501 の RAM 2511 にも格納される。

これにより、メモリカード 2502 に書き出された暗号化コンテンツのうち、携帯電話機 2501 によって書き出された暗号化コンテンツ 2505 は、そのディレクトリ名 2513 によって、携帯電話機 2501 において判別することができる状態となる。

10 また、メモリカード 2502 の所定のディレクトリ 2503 に格納された暗号化コンテンツ 2505 を携帯電話機 2501 に読み込む場合、携帯電話機 2501 のメモリ読込プログラム 108 は、暗号化コンテンツ 2505 を読み込む処理に先立って、携帯電話機 2501 の RAM 2511 に格納されているディレクトリ名 2513 と一致するディレクトリ名がメモリカード 2502 の
15 ディレクトリに存在するか否かを判断し、一致するディレクトリ名 2513 が存在する場合には、そのディレクトリを一覧情報化する。この一覧に載せられたディレクトリの暗号化コンテンツ 2505 は、携帯電話機 2501 によってメモリカード 2502 に書き出されたものであると判別することができる。

このように、メモリカード 2502 に設定されているディレクトリ 2503
20 が、携帯電話機 2501 によってメモリカード 2502 に設定されたものであることが判ると、暗号化/復号化プログラム 2509 は、当該ディレクトリ名 2513 がつけられたディレクトリ 2503 に格納されている暗号化コンテンツ 2505 を復号化し、当該復号化されたコンテンツ 2512 を RAM 2511 に格納する。

25 図 27 は、携帯電話機 2501 の RAM 2511 に格納されているコンテンツ 2512 を、メモリカード 2502 に格納する際の、暗号化/復号化プログラム 2509 の処理手順を示すフロー図である。

図27に示すように、暗号化/復号化プログラム2509は、ステップST2601において、まず、コンテンツ格納用のディレクトリ2503を作成した後、続くステップST2602に移って、RAM2511からコンテンツ2512を取得する。そして、暗号化/復号化プログラム2509は、ステップST2603に移って、ステップST2602において取得したコンテンツ2512を、ROM2514内の端末識別子2515を用いて例えばトリプルDES暗号方式で暗号化する。

そして、暗号化/復号化プログラム2509は、ステップST2604に移って、ステップST2603において暗号化された暗号化コンテンツ2505を、
10 ステップST2601において作成された、メモ리카ード2502のディレクトリ2503に格納する。

このときステップST2601において作成された暗号化コンテンツ2505の格納先であるディレクトリ2503のディレクトリ名2513は、ステップST2605において、暗号化/復号化プログラム2509によって携帯電話
15 2501のRAM2511に格納される。

これにより、図28に示すように、メモ리카ード2502においては、暗号化コンテンツ2505が、携帯電話機2501のRAM2511に格納されたディレクトリ名2513と同じディレクトリ名のディレクトリ2503に格納された状態となる。

20 また、図29は、図27の処理手順によってメモ리카ード2502に格納された暗号化コンテンツ2505を携帯電話機2501によって読み込んで復号化する際の、暗号化/復号化プログラム2509とコンテンツ格納ディレクトリ判別プログラム2510との処理手順を示すフロー図である。

図29に示すように、コンテンツ格納ディレクトリ判別プログラム2510
25 は、ステップST2801において、メモ리카ード2502内に暗号化コンテンツがあるか否かを調べる。ここで肯定結果が得られると、このことは、携帯電話機2501によってメモ리카ード2502に書き出された暗号化コンテ

ンツ、すなわち携帯電話機2501によって利用可能な暗号化コンテンツ2505がメモ리카ード2502に格納されている可能性があることを意味しており、このとき、コンテンツ格納ディレクトリ判別プログラム2510は、ステップST2802に移って、暗号化コンテンツが格納されているディレクトリ名を取得する。

そして、コンテンツ格納ディレクトリ判別プログラム2510は、ステップST2803に移って、ステップST2802において取得したディレクトリ名が、携帯電話機2501のRAM2511に格納されているディレクトリ名2513と同一であるか否かを判断する。

10 ここで否定結果が得られると、このことは、このとき取得したディレクトリ名が、携帯電話機2501によって作成されメモ리카ード2501に設定されたものではないこと、すなわち、このディレクトリ名が付けられたディレクトリに格納されている暗号化コンテンツが、携帯電話機2501によってメモ리카ード2502に書き出されたものではないことを意味しており、このとき、
15 コンテンツ格納ディレクトリ判別プログラム2510は、上述のステップST2801に戻って、メモ리카ード2502に他の暗号化コンテンツが格納されているか否かを判断し、当該判断結果に基づいて上述の場合と同様の処理を行う。

これに対して、ステップST2803において肯定結果が得られると、この
20 ことは、このとき取得したディレクトリ名が、携帯電話機2501によって作成されメモ리카ード2501に設定されたディレクトリ名2513であること、すなわち、このディレクトリ名2513が付けられたディレクトリ2503に格納されている暗号化コンテンツ2505が、携帯電話機2501によってメモ리카ード2502に書き出されたものであることを意味しており、この
25 とき、コンテンツ格納ディレクトリ判別プログラム2510は、ステップST2804に移って、当該ディレクトリ名2513を一覧情報に追加した後、上述のステップST2801に戻って、メモ리카ード2502に他の暗号化コン

テンツが格納されているか否かを判断し、当該判断結果に基づいて上述の場合と同様の処理を行う。

そして、メモ리카ード2502に格納されている暗号化コンテンツ（ディレクトリ名）のすべてについて、携帯電話機2501によって書き出されたものであるか否かの判断が完了すると、コンテンツ格納ディレクトリ判別プログラム2510は、ステップST2801において否定結果を得ることにより、ステップST2805に移って、上述のステップST2804において作成された一覧情報によって特定される暗号化コンテンツ2505に関する情報（ディレクトリ名等）を液晶画面116に一覧表示する。

10 これにより、液晶画面116には、メモ리카ード2502に格納されている暗号化コンテンツのうち、携帯電話機2501によって利用可能な暗号化コンテンツ2505に関連する情報が一覧表示される。

因みに、携帯電話機2501によって利用可能な暗号化コンテンツ2505に関する情報を一覧表示する構成としては、暗号化コンテンツ2505をメモ리카ード2502に格納する際に、その暗号化コンテンツ2505に対応した
15 タイトル等の簡易情報のみを携帯電話機2501のRAM2511に格納し、ステップST2803における一致結果に基づいて、当該格納されている簡易情報を一覧表示する等の方法も考えられる。

ステップST2805において、液晶画面116にコンテンツの一覧が表示
20 されると、利用者は、入力インターフェイス117を操作することにより、当該表示された一覧のなかから所望とするコンテンツを選択する。

これにより、暗号化/復号化プログラム2509は、ステップST2806に移って、メモリ読込プログラム108を用いて、このとき入力インターフェイス117を介して指定された暗号化コンテンツ2505をメモ리카ード25
25 02から読み込み、さらに続くステップST2807に移って、ステップST2806においてメモ리카ード2502から取得した暗号化コンテンツ2505を、ROM2514に格納されている端末識別子2515を用いて復号化

し、RAM 2511に格納する。

RAM 2511に格納されたコンテンツ 2512は、携帯電話機 2501の利用者が入力インターフェイス 117を操作することにより起動され、利用者の利用に供される。

- 5 以上の構成において、携帯電話機 2501は、メモリカード 2502に暗号化コンテンツ 2505を書き出す際に、そのメモリカード 2502での格納先であるディレクトリ 2503のディレクトリ名 2513をRAM 2513に格納しておく。これにより、携帯電話機 2501においては、当該携帯電話機 2501においてのみ使用可能な暗号化コンテンツ 2505が格納されたディレクトリ 2503のディレクトリ名 2513が、自身の環境に設定された状態となる。

- そして、この設定されたディレクトリ名 2513が付けられた、メモリカード 2502のディレクトリ 2503に、暗号化コンテンツ 2505が格納される。これにより、ディレクトリ名 2513は、暗号化コンテンツ 2505の利用環境（利用可能な携帯電話機 2501）を識別するための情報として利用可能な状態となる。

- このように、暗号化コンテンツ 2505をメモリカード 2502に書き出す際のディレクトリ名 2513は、携帯電話機 2501が暗号化コンテンツ 2505をメモリカード 2502に書き出したことの事実を表わすキーワードとして携帯電話機 2501及びメモリカード 2502の双方に格納される。

- 従って、携帯電話機 2501に装着されたメモリカード 2502に、当該携帯電話機 2501に格納されているディレクトリ名 2513と同一のディレクトリ名が設定されている場合には、当該ディレクトリ名 2513が付けられたディレクトリ 2503に格納されている暗号化コンテンツ 2505は、携帯電話機 2501によって書き出されたもの、すなわち、携帯電話機 2501によって利用が可能なコンテンツであることを意味する。

従って、メモリカード 2502のディレクトリ名と、携帯電話機 2501に

格納されているディレクトリ名 2513 とが一致した場合、このディレクトリ名 2513 が付けられた、メモ리카ード 2502 のディレクトリ 2503 に格納されている暗号化コンテンツ 2505 は、携帯電話機 2501 に読み込んで、当該携帯電話機 2501 によって利用することが可能であり、この一致結果を
5 受けて、携帯電話機 2501 の暗号化/復号化プログラム 2509 は、メモ리카ード 2502 から当該暗号化コンテンツ 2505 を読み込み、当該読み込まれた暗号化コンテンツ 2505 を復号化する。

このように、メモ리카ード 2502 のディレクトリ名が、RAM 2511 に格納されているディレクトリ名 2513 と一致することを条件に、当該ディレ
10 クトリ名 2513 が付けられた、メモ리카ード 2502 のディレクトリ 2503 に格納されている暗号化コンテンツ 2505 をメモ리카ード 2502 から携帯電話機 2501 に読み込んで復号化することにより、携帯電話機 2501 は、当該携帯電話機 2501 において利用可能である暗号化コンテンツ 2505 のみを、データ量の少ないディレクトリ名 2113 に基づいて選択すること
15 ができる。

従って、メモ리카ード 2502 に複数の暗号化コンテンツが格納されている状態であって、これら複数の暗号化コンテンツを利用可能な端末装置（携帯電話機等）が各暗号化コンテンツ毎に異なる場合であっても、携帯電話機 2501 は、これら複数のデータ量の多い暗号化コンテンツをすべて復号化する必要
20 はなく、当該複数の暗号化コンテンツにそれぞれ対応付けられた、データ量の少ないディレクトリ名 2513 を取得するだけで、利用可能な暗号化コンテンツ 2505 を判別することができる。

このように、本実施の形態のコンテンツ処理装置としての携帯電話機 2501 によれば、コンテンツ蓄積媒体であるメモ리카ード 2502 に格納された複
25 数の暗号化コンテンツの判別を一段と容易に行うことが可能となり、携帯電話機 2501 において利用可能な暗号化コンテンツ 2505 を一段と迅速に復号化することができる。

なお、この実施の形態においては、暗号化コンテンツ 2505 を判別するための情報として、当該暗号化コンテンツ 2505 をメモ리카ード 2502 に書き出す際のディレクトリ名 2513 を携帯電話機 2501 において自動的に作成する場合について述べたが、これに限らず、利用者が自ら入力インターフェイス 117 を操作して入力した設定情報、または携帯電話機 2501 が乱数等を用いてランダムに設定した値等を用いるようにしてもよい。また、このようにして作成されたディレクトリ名 2513 は、上述の実施の形態のディレクトリ名 2513 の場合を含めて、暗号化してメモ리카ード 2502 のディレクトリ名として設定するようにしてもよい。このようにすれば、暗号化コンテンツ 2505 を判別するための、携帯電話機 2501 によって作成されたディレクトリ名が、メモ리카ード 2502 から第三者に知られた場合であっても、暗号化コンテンツ 2505 が不正に復号化されることを防止することができる。

また、この実施の形態の携帯電話機 2501 においては、端末識別子 2515 として、その携帯電話機 2501 の電話番号を用いる場合について述べたが、これに限らず、例えば携帯電話機 2501 の製造番号のようなその携帯電話機 2501 を識別するための識別子、又は、その他の何らかの意味を持つ文字列、数値、画像または音声等のデータ、若しくは特定のサービスと契約したことを示す識別子（会員番号等）を用いるようにしてもよい。また、この端末識別子 2515 として電話番号、製造番号、又はその他の文字列等の情報そのものではなく、端末識別子に対してある変換を加えた結果（端末識別子に関連する情報）を用いるようにしてもよい。このようにすれば、端末識別子によってコンテンツ及び特定データを暗号化する際の暗号化方法、及び端末識別子が第三者に漏洩した場合であっても、その端末識別子は、暗号化鍵となり得る他のデータに変換されていることにより、このデータ（暗号化鍵）によって暗号化された暗号化コンテンツ及び暗号化特定データが解読されることを防止することができる。

また、この実施の形態においては、携帯電話機 2501 の RAM 2511 に、

メモ리카ード2502のディレクトリ名2513を格納し、当該携帯電話機1501によって利用可能な暗号化コンテンツ2505を、当該ディレクトリ名2513によって判別する場合について述べたが、これに限らず、メモ리카ード2502に固有のカード識別子を、携帯電話機2501のRAM2511と
5 メモ리카ード2502の双方によって共有し、当該カード識別子及びそのディレクトリ名2513の両方によって、利用可能な暗号化コンテンツ2505を判別するようにしてもよい。このようにすれば、複数のメモ리카ードをコンテンツの種類（オーディオ用、ゲーム用、等）ごとに使い分ける場合に対応することができる。また、このようにすれば、同じディレクトリ名を有する異なる
10 メモ리카ードについても、これらのメモ리카ードに格納されている各暗号化コンテンツを利用可能であるか否かを判別することができる。

また、この実施の形態においては、コンテンツを格納するコンテンツ蓄積媒体としてメモ리카ード2502を用いる場合について述べたが、これに限らず、要はデジタル情報化されたコンテンツを格納可能なコンテンツ蓄積媒体であ
15 れば、他のデバイスを広く適用することができる。

（実施の形態8）

上述の実施の形態1～実施の形態7においては、1つの携帯電話機において、メモ리카ードに格納されている複数の暗号化コンテンツのなかから自身で利用可能なコンテンツを判別する場合について述べたが、本発明はこれに限らず、
20 1つのメモ리카ードを異なる携帯電話機に差し替えて、これら複数の携帯電話機において当該1つのメモ리카ードを利用する場合においても、適用することができる。

この場合、携帯電話機のROMに格納される端末識別子として、1つのメモ리카ードの利用を共有する複数の携帯電話機において共通の端末識別子を格
25 納しておく。このようにすれば、特定の識別子を持つ環境を複数の携帯電話機に設定することができ、1つのメモ리카ードを複数の携帯電話機を含む環境で利用することが可能となる。

以上説明したように、本発明によれば、コンテンツ蓄積媒体に格納された暗号化コンテンツについて、当該暗号化コンテンツに関連したデータ量の少ない情報を当該暗号化コンテンツに対応付けてコンテンツ蓄積媒体に格納することにより、データ量の多い暗号化コンテンツを復号化することなく、関連した

5 情報に基づいて暗号化コンテンツを容易に判別することができる。

また、本発明によれば、コンテンツ蓄積媒体に格納されているコンテンツが使用可能であるか否かを判断することが可能となることにより、正規のデータでないデータを誤って再生してしまうといった不都合を防止することができる。

10 本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報の前記コンテンツ蓄積媒体への書き込みを行うコンテンツ処理装置であって、前記識別子又は前記識別子に関連する情報を暗号化の鍵として特

15 定のデータを暗号化するデータ暗号化部と、前記暗号化された特定のデータを前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する暗号化データ格納部と、を具備する構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記暗号化データ格納部は、前記暗号化された特定のデータの前記コンテンツ蓄積媒体上の格納先と

20 して、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納するとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された特定のデータとの関連付けを行なう構成を採る。

この構成によれば、コンテンツ蓄積媒体の認証領域にアクセス可能な場合に

25 のみ暗号化コンテンツの判別を行うことができる。

本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用

を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報の前記コンテンツ蓄積媒体への書き込みを行うコンテンツ処理装置であって、前記識別子を前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する識別子格納部、を具備する構成を採る。

- 5 本発明のコンテンツ処理装置は、上記構成において、前記識別子格納部は、前記識別子の前記コンテンツ蓄積媒体上の格納先として、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納するとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された識別子との関連付けを行なう構成を採る。

- 10 本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記蓄積媒体に書き込むコンテンツ処理装置であって、特定の暗号化手段を用いて前記識別子を暗号化する識別子暗号化部と、前記暗号化された識別子を前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する暗号化識別子格納部と、を具備する構成を採る。

- 15 本発明のコンテンツ処理装置は、上記構成において、前記暗号化識別子格納部は、前記暗号化識別子の前記コンテンツ蓄積媒体上の格納先として、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納し、同時に前記デジタル情報のファイルと前記認証ファイルシステム内に格納された暗号化識別子との関連付けを行なう構成を採る。

- 20 本発明のコンテンツ処理装置は、上記構成において、前記コンテンツ処理装置は、さらに、前記識別子を特定の変換式に対応して変換する識別子変換部を具備し、前記識別子暗号化部は、前記識別子変換部によって変換された識別子を暗号化し、前記暗号化識別子格納部は、当該暗号化された識別子を前記コン

テンツ蓄積媒体に格納する構成を採る。

本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理装置であつて、前記識別子とは異なる、前記特定の識別子を持つ環境に固有な特定のデータを、前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する固有データ格納部を具備する構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記固有データ格納部は、前記特定のデータの前記コンテンツ蓄積媒体上の格納先として、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納するとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された前記特定のデータとの関連付けを行なう構成を採る。

本発明のコンテンツ処理装置は、デジタル情報を着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理装置であつて、前記デジタル情報を前記コンテンツ蓄積媒体に書き込んだ時刻を特定する書き込み時刻特定部と、前記特定された時刻を、書き込みを行なう自身の環境に格納するとともに、前記デジタル情報のファイルと関連付けた上で前記コンテンツ蓄積媒体に格納する書き込み時刻格納部とを具備する構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記書き込み時刻格納部は、前記書き込み時刻の前記コンテンツ蓄積媒体上の格納先として、前記着脱可能なコンテンツ蓄積媒体と前記特定の環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納するとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された前

記書き込み時刻との関連付けを行なう構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記情報管理システムは、特定の識別子を持つ環境でのみ前記デジタル情報の利用を許可するものであって、前記コンテンツ処理装置は、さらに、前記書き込み時刻を前記識別子
5 に関連する情報を用いて暗号化する書き込み時刻暗号化部を備え、前記書き込み時刻格納部は、少なくともコンテンツ蓄積媒体に格納する書き込み時刻を、前記書き込み時刻暗号化部によって暗号化されたものとする構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記コンテンツ処理装置は、さらに、前記識別子に関連する情報を利用して前記書き込み時刻を変換
10 する書き込み時刻変換部を具備し、前記書き込み時刻暗号化部は、前記変換された書き込み時刻を特定の方法で暗号化する構成を採る。

本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を
15 前記コンテンツ蓄積媒体に書き込むコンテンツ処理装置であって、ユーザが指定する値あるいは名称であるユーザ指定値を環境に設定するユーザ指定値書き込み部と、前記ユーザ指定値を前記コンテンツ蓄積媒体に格納するユーザ指定値格納部とを備える構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記コンテンツ処理装置は、さらに、ユーザがユーザ指定値を指定していない状態でユーザ指定値として利用するための初期値をランダムに設定する、初期値設定部を具備する構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記情報管理システムは、特定の識別子を持つ環境でのみ前記デジタル情報の利用を許可するものであって、前記コンテンツ処理装置は、さらに、前記ユーザ指定値を前記識別子
25 に関連する情報を用いて暗号化するユーザ指定値暗号化部を具備し、前記ユーザ指定値格納部は、前記コンテンツ蓄積媒体に格納するユーザ指定値を、前記

ユーザ指定値暗号化部によって暗号化されたものとする構成を採る。

本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を

5 前記コンテンツ蓄積媒体に書き込むコンテンツ処理装置であって、前記デジタル情報を前記コンテンツ蓄積媒体に書き込む際に特定のデータを作成する書き込み特定データ生成部と、前記特定のデータを、書き込みを行なう自身の環境に格納するとともに、前記デジタル情報のファイルと関連付けた上で前記コンテンツ蓄積媒体に格納する書き込み特定データ格納部と、を具備する構成を

10 採る。

本発明のコンテンツ処理装置は、上記構成において、前記書き込み特定データ生成部において、前記特定のデータは、書き込みの際にランダムに生成されるか、あるいは特定の手順によって生成される構成を採る。

本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理装置であって、前記デジタル情報を前記コンテンツ蓄積媒体に書き込んだ際の書き込み箇所を特定する書き込み箇所特定部と、前記特定された箇所を、書き込みを行なう自身の環境

20 に格納する書き込み箇所格納部と、を具備する構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記デジタル情報は、前記識別子に関連する情報を利用して暗号化されている構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記特定のデータは、なんらかの意味を持つ文字列、数値、画像、音声等のデータである構成を採る。

25 本発明のコンテンツ処理装置は、上記構成において、前記識別子は、なんらかの意味を持つ文字列、数値、画像、音声等のデータである構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記特定の環境または

特定の識別子を持つ環境は、前記着脱可能なコンテンツ蓄積媒体を着脱することのできる特定の機器である構成を採る。

- 本発明のコンテンツ処理装置は、上記構成において、前記特定の環境または特定の識別子を持つ環境は、特定のサービスと契約したことを示す識別子によって特定される環境である構成を採る。

- 以上の構成によれば、コンテンツ蓄積媒体に格納された複数の暗号化コンテンツの判別を、当該暗号化コンテンツに関連付けられた情報に基づいて、一段と容易に行うようにすることができる。また、コンテンツ蓄積媒体に格納されているコンテンツが使用可能であるか否かを判断することが可能となり、正規のデータでないデータを誤って再生してしまうといった不都合を防止することができる。

- 本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理装置であって、前記コンテンツ蓄積媒体上に格納された前記デジタル情報のファイルと関連付けて格納された暗号化データを読み出す暗号化データ読み出し部と、前記読み出された暗号化データを自身の環境の識別子に関連する情報によって復号化し、特定のデータと合致するかどうかを判定する暗号化データ判別部と、を具備する構成を採る。

- 本発明のコンテンツ処理装置は、上記構成において、前記暗号化データ読み出し部は、前記暗号化された特定のデータを、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる、前記コンテンツ蓄積媒体上の認証ファイルシステム内から読み出す構成を採る。

本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用

を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理装置であって、前記コンテンツ蓄積媒体上に格納された前記デジタル情報のファイルと関連付けて格納された識別子を読み出し、自身の環境の識別子と合致するかど

5 うかを判定する識別子判別部、を具備する構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記識別子判別部は、前記識別子を、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる、前記コンテンツ蓄積媒体上の認証ファイルシステム内から読み出す構成を採る。

10 本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理装置であって、前記コンテンツ蓄積媒体上に格納された前記デジタル情報のファイルと
15 関連付けて格納された暗号化識別子を読み出す暗号化識別子読み出し部と、前記読み出された暗号化識別子を自身の環境の特定の復号化手段によって復号化し、自身の識別子と合致するかどうかを判定する暗号化識別子判別部と、を具備する構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記暗号化識別子読み
20 出し部は、前記暗号化識別子を、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる、前記コンテンツ蓄積媒体上の認証ファイルシステム内から読み出す構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記コンテンツ処理装
25 置は、さらに、前記暗号化識別子を特定の変換式に対応して変換する識別子逆変換部を具備し、前記暗号化識別子判別部は、復号化した暗号化識別子を前記識別子逆変換部で逆変換してから自身の識別子と合致するかどうかを判定す

る構成を採る。

- 本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理装置であって、前記コンテンツ蓄積媒体上に格納された前記デジタル情報のファイルと関連付けて格納された固有データを読み出す固有データ読み出し部と、前記読み出された固有データを自身の環境の固有データと合致するかどうかを判定する固有データ判別部と、を具備する構成を採る。
- 10 本発明のコンテンツ処理装置は、上記構成において、前記固有データ読み出し部は、前記固有データを、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる、前記コンテンツ蓄積媒体上の認証ファイルシステム内から読み出す構成を採る。
- 15 本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理装置であって、前記コンテンツ蓄積媒体上に格納された、前記デジタル情報のファイルと関連付けられた前記デジタル情報の書き込み時刻を読み出す書き込み時刻読み出し部と、前記読み出された書き込み時刻と、自身の環境に格納されている書き込み時刻のひとつとが合致するか否かを判定する書き込み時刻判別部と、を具備する構成を採る。
- 20 本発明のコンテンツ処理装置は、前記書き込み時刻読み出し部は、前記書き込み時刻を、前記着脱可能なコンテンツ蓄積媒体と前記特定の環境との間での認証が成功した場合にのみアクセスが可能となる、前記コンテンツ蓄積媒体上の認証ファイルシステム内から読み出す構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記情報管理システムは、特定の識別子を持つ環境でのみ前記デジタル情報の利用を許可するものであって、前記書き込み時刻判別部は、前記書き込み時刻読み出し部で読み出された書き込み時刻を、自身の環境の持つ識別子に関連する情報を用いて復号してから自身の環境に格納されている書き込み時刻のひとつと合致するか否かを判定する構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記コンテンツ処理装置は、さらに、前記書き込み時刻読み出し部で読み出された書き込み時刻を、前記識別子に関連する情報を利用して変換する書き込み時刻変換部を具備し、前記書き込み時刻判別部は、前記変換された書き込み時刻を特定の方法で復号してから自身の環境に格納されている書き込み時刻のひとつと合致するか否かを判定する構成を採る。

本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理装置であって、前記コンテンツ蓄積媒体上に格納された、前記デジタル情報のファイルと関連付けられた、ユーザによって指定されたユーザ指定値を読み出すユーザ指定値読み出し部と、前記読み出されたユーザ指定値と、自身の環境に格納されているユーザ指定値が合致するか否かを判定するユーザ指定値判別部と、を具備する構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記情報管理システムは、特定の識別子を持つ環境でのみ前記デジタル情報の利用を許可するものであって、前記ユーザ指定値判別部は、前記ユーザ指定値読み出し部で読み出されたユーザ指定値を、自身の環境の持つ識別子に関連する情報を用いて復号してから自身の環境に格納されているユーザ指定値と合致するか否かを判定する構成を採る。

本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理装置であって、前記コンテンツ蓄積媒体上に格納された、前記デジタル情報のファイルと関連付けられた特定のデータを読み出す書き込み特定データ読み出し部と、前記読み出された特定のデータと、自身の環境に格納されている特定のデータのひとつと合致するか否かを判定する書き込み特定データ判別部と、を具備する構成を採る。

本発明のコンテンツ処理装置は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理装置であって、前記コンテンツ蓄積媒体上に格納された、前記デジタル情報のファイルの格納箇所である書き込み箇所を前記コンテンツ蓄積媒体上から読み出す書き込み箇所読み出し部と、前記読み出された書き込み箇所と、自身の環境に格納されている書き込み箇所のひとつと合致するか否かを判定する書き込み箇所判別部と、を具備する構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記特定の環境または特定の識別子を持つ環境は、前記着脱可能なコンテンツ蓄積媒体を着脱することのできる特定の機器である構成を採る。

本発明のコンテンツ処理装置は、上記構成において、前記特定の環境または特定の識別子を持つ環境は、特定のサービスと契約したことを示す識別子によって特定される環境である構成を採る。

以上の構成によれば、コンテンツ蓄積媒体に格納された暗号化コンテンツを読み出し、復号化する前に、当該暗号化コンテンツに関連付けられた情報を基に、暗号化コンテンツを判別することにより、暗号化コンテンツを復号化することなく、その内容を容易に判別することができる。また、コンテンツ蓄積媒

体に格納されているコンテンツが使用可能であるか否かを判断することが可能となり、正規のデータでないデータを誤って再生してしまうといった不都合を防止することができる。

本発明のコンテンツ蓄積媒体は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる前記コンテンツ蓄積媒体であって、前記識別子又は前記識別子に関連する情報を暗号化の鍵として暗号化された特定のデータが、前記デジタル情報のファイルと関連付けられて格納されている構成を採る。

10 本発明のコンテンツ蓄積媒体は、上記構成において、前記コンテンツ蓄積媒体は、さらに、前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステムを具備し、前記暗号化された特定のデータは、前記認証ファイルシステム内に格納されているとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された特定
15 のデータとの関連付けが記録されている構成を採る。

本発明のコンテンツ蓄積媒体は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる前記コンテンツ蓄積媒体であって、前記識別子が前記デジタル情報のファ
20 イルと関連付けて格納されている構成を採る。

本発明のコンテンツ蓄積媒体は、上記構成において、前記コンテンツ蓄積媒体は、さらに、前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステムを具備し、前記識別子は、前記認証ファイルシステム内に格納されているとともに、前記デジタル情報のフ
25 ァイルと前記認証ファイルシステム内に格納された識別子との関連付けが記録されている構成を採る。

本発明のコンテンツ蓄積媒体は、デジタル情報化されたコンテンツを着脱可

能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる前記コンテンツ蓄積媒体であって、特定の暗号化手段を用いて暗号化された前記識別子が、前記デジタル情報のファイルと関連付けて格納されている構成を採る。

本発明のコンテンツ蓄積媒体は、上記構成において、前記コンテンツ蓄積媒体は、さらに、前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステムを具備し、前記暗号化識別子は、前記認証ファイルシステム内に格納されているとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された暗号化識別子との関連付けが記録されている構成を採る。

本発明のコンテンツ蓄積媒体は、上記構成において、前記識別子は、特定の変換式に対応して変換された上で前記特定の暗号化手段を用いて暗号化されている構成を採る。

本発明のコンテンツ蓄積媒体は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる前記コンテンツ蓄積媒体であって、前記識別子とは異なる、前記特定の識別子を持つ環境に固有な特定のデータが、前記デジタル情報のファイルと関連付けられて格納されている構成を採る。

本発明のコンテンツ蓄積媒体は、上記構成において、前記コンテンツ蓄積媒体は、さらに、前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステムを具備し、前記固有の特定データは、前記認証ファイルシステム内に格納されているとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された前記固有の特定データとの関連付けが記録されている構成を採る。

本発明のコンテンツ蓄積媒体は、デジタル情報化されたコンテンツを着脱可

能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて用いられる前記コンテンツ蓄積媒体であって、前記デジタル情報が書き込まれた時刻を特定する書き込み時刻が、前記デジタル情報のファイルと関連付けられた上で格納されている構成を採る。

本発明のコンテンツ蓄積媒体は、上記構成において、前記コンテンツ蓄積媒体は、さらに、前記特定の環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステムを具備し、前記書き込み時刻は、前記認証ファイルシステム内に格納されているとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された前記書き込み時刻との関連付けが記録されている構成を採る。

本発明のコンテンツ蓄積媒体は、上記構成において、前記情報管理システムは、特定の識別子を持つ環境でのみ前記デジタル情報の利用を許可するものであって、前記書き込み時刻は前記識別子に関連する情報を用いて暗号化されて格納されている構成を採る。

本発明のコンテンツ蓄積媒体は、上記構成において、前記書き込み時刻は、前記識別子に関連する情報を利用して変換されたのち、特定の方法で暗号化されている構成を採る。

本発明のコンテンツ蓄積媒体は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて用いられる前記コンテンツ蓄積媒体であって、ユーザが環境に対して指定する値あるいは名称であるユーザ指定値が、前記デジタル情報のファイルと関連付けられた上で格納されている構成を採る。

本発明のコンテンツ蓄積媒体は、上記構成において、前記ユーザ指定値としては、ユーザがユーザ指定値を指定していない状態では、初期値としてランダムな値が格納されている構成を採る。

本発明のコンテンツ蓄積媒体は、上記構成において、前記情報管理システムは、特定の識別子を持つ環境でのみ前記デジタル情報の利用を許可するものであって、前記ユーザ指定値は前記識別子に関連する情報を用いて暗号化されて格納されている構成を採る。

- 5 本発明のコンテンツ蓄積媒体は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて用いられる前記コンテンツ蓄積媒体であって、前記デジタル情報が書き込まれる際に生成された特定のデータが、前記デジタル情報のファイルと関連付けられた上で格納されて
- 10 いる構成を採る。

本発明のコンテンツ蓄積媒体は、上記構成において、前記特定のデータは、書き込みの際にランダムに生成されるか、あるいは特定の手順によって生成されて格納されている構成を採る。

- 本発明のコンテンツ蓄積媒体は、上記構成において、前記デジタル情報は、
- 15 前記識別子に関連する情報を利用して暗号化されている構成を採る。

本発明のコンテンツ蓄積媒体は、上記構成において、前記特定のデータは、なんらかの意味を持つ文字列、数値、画像、音声等のデータである構成を採る。

本発明のコンテンツ蓄積媒体は、上記構成において、前記識別子は、なんらかの意味を持つ文字列、数値、画像、音声等のデータである構成を採る。

- 20 本発明のコンテンツ蓄積媒体は、上記構成において、前記識別子は、特定のサービスと契約したことを示すデータである構成を採る。

- 以上の構成によれば、コンテンツ蓄積媒体において、暗号化コンテンツに関連付けられた情報が格納されることにより、当該情報に基づいて、暗号化コンテンツの判別を一段と容易に行わせることができる。また、この情報によって、
- 25 コンテンツ蓄積媒体に格納されているコンテンツが使用可能であるか否かを端末装置等の使用環境に判断させることが可能となり、当該使用環境が正規のデータでないデータを誤って再生してしまうといった不都合を防止すること

ができる。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報の前記コンテンツ蓄積媒体への書き込みを行うコンテンツ処理方法であって、前記識別子に関連する情報を暗号化の鍵として特定のデータを暗号化するデータ暗号化ステップと、前記暗号化された特定のデータを前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する暗号化データ格納ステップと、を具備するようにした。

10 本発明のコンテンツ処理方法は、上記方法において、前記暗号化データ格納ステップでは、前記暗号化された特定のデータの前記コンテンツ蓄積媒体上の格納先として、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納されるとともに、前記デジタル情報のファイルと前記認証
15 ファイルシステム内に格納された特定のデータとの関連付けが行なわれるようにした。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報の前記コンテンツ蓄積媒体への書き込みを行うコンテンツ処理方法であって、前記識別子を前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する識別子格納ステップを具備するようにした。

20 本発明のコンテンツ処理方法は、上記方法において、前記識別子格納ステップは、前記識別子の前記コンテンツ蓄積媒体上の格納先として、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納されるとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納
25

された識別子との関連付けが行なわれるようにした。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記蓄積媒体に書き込むコンテンツ処理方法であって、特定の暗号化手段を用いて前記識別子を暗号化する識別子暗号化ステップと、前記暗号化された識別子を前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する暗号化識別子格納ステップと、を備えるようにした。

本発明のコンテンツ処理方法は、上記方法において、前記暗号化識別子格納ステップでは、前記暗号化識別子の前記コンテンツ蓄積媒体上の格納先として、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納されるとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された暗号化識別子との関連付けが行なわれるようにした。

本発明のコンテンツ処理方法は、上記方法において、前記コンテンツ処理方法は、さらに、前記識別子を特定の変換式に対応して変換する識別子変換ステップを具備し、前記識別子暗号化ステップでは、前記識別子変換ステップによって変換された識別子が暗号化され、前記暗号化識別子格納ステップでは、当該暗号化された識別子が前記コンテンツ蓄積媒体に格納されるようにした。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理方法であって、前記識別子とは異なる、前記特定の識別子を持つ環境に固有な特定のデータを、前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する固有データ格納ステップを備えるようにした。

本発明のコンテンツ処理方法は、上記方法において、前記固有データ格納ス

- テップでは、前記特定のデータの前記コンテンツ蓄積媒体上の格納先として、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納されるとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された前記特定のデータとの関連付けが行なわれるようにした。

- 本発明のコンテンツ処理方法は、デジタル情報を着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理方法であって、前記デジタル情報を前記コンテンツ蓄積媒体に書き込んだ時刻を特定する書き込み時刻特定ステップと、前記特定された時刻を、書き込みを行なう自身の環境に格納するとともに、前記デジタル情報のファイルと関連付けた上で前記コンテンツ蓄積媒体に格納する書き込み時刻格納ステップと、を具備するようにした。

- 本発明のコンテンツ処理方法は、上記方法において、前記書き込み時刻格納ステップでは、前記書き込み時刻の前記コンテンツ蓄積媒体上の格納先として、前記着脱可能なコンテンツ蓄積媒体と前記特定の環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納されるとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された前記書き込み時刻との関連付けが行なわれるようにした。

- 本発明のコンテンツ処理方法は、上記方法において、前記情報管理システムは、特定の識別子を持つ環境でのみ前記デジタル情報の利用を許可するものであって、前記コンテンツ処理方法は、さらに、前記書き込み時刻を前記識別子に関連する情報を用いて暗号化する書き込み時刻暗号化ステップを備え、前記書き込み時刻格納ステップでは、少なくともコンテンツ蓄積媒体に格納する書き込み時刻が、前記書き込み時刻暗号化部によって暗号化されたものとなるようにした。

本発明のコンテンツ処理方法は、上記方法において、前記コンテンツ処理方

法は、さらに、前記識別子に関連する情報を利用して前記書き込み時刻を変換する書き込み時刻変換ステップを具備し、前記書き込み時刻暗号化ステップでは、前記変換された書き込み時刻が特定の方法で暗号化されるようにした。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理方法であって、ユーザが指定する値あるいは名称であるユーザ指定値を環境に設定するユーザ指定値書き込みステップと、前記ユーザ指定値を前記コンテンツ蓄積媒体に格納するユーザ指定値格納ステップと、を具備するようにした。

本発明のコンテンツ処理方法は、上記方法において、さらに、ユーザがユーザ指定値を指定していない状態でユーザ指定値として利用するための初期値をランダムに設定する、初期値設定ステップを具備するようにした。

本発明のコンテンツ処理方法は、上記方法において、前記情報管理システムは、特定の識別子を持つ環境でのみ前記デジタル情報の利用を許可するものであって、前記コンテンツ処理方法は、さらに、前記ユーザ指定値を前記識別子に関連する情報を用いて暗号化するユーザ指定値暗号化ステップを具備し、前記ユーザ指定値格納ステップでは、前記コンテンツ蓄積媒体に格納するユーザ指定値が、前記ユーザ指定値暗号化部によって暗号化されたものとなるようにした。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理方法であって、前記デジタル情報を前記コンテンツ蓄積媒体に書き込む際に特定のデータを作成する書き込み特定データ生成ステップと、前記特定のデータを、書き込みを行なう自身の環境に格納するとともに、前記デジタル情報のファイルと関連付けた上で

前記コンテンツ蓄積媒体に格納する書き込み特定データ格納ステップと、を具備するようにした。

- 本発明のコンテンツ処理方法は、上記方法において、前記書き込み特定データ生成ステップにおいて、前記特定のデータは、書き込みの際にランダムに生成されるか、あるいは特定の手順によって生成されるようにした。

- 本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理方法であって、前記デジタル情報を前記コンテンツ蓄積媒体に書き込んだ際の書き込み箇所を特定する書き込み箇所特定ステップと、前記特定された箇所を、書き込みを行なう自身の環境に格納する書き込み箇所格納ステップと、を具備するようにした。

本発明のコンテンツ処理方法は、上記方法において、前記デジタル情報は、前記識別子に関連する情報を利用して暗号化されているようにした。

- 本発明のコンテンツ処理方法は、上記方法において、前記特定のデータは、なんらかの意味を持つ文字列、数値、画像、音声等のデータであるようにした。

本発明のコンテンツ処理方法は、上記方法において、前記識別子は、なんらかの意味を持つ文字列、数値、画像、音声等のデータであるようにした。

- 本発明のコンテンツ処理方法は、上記方法において、前記特定の環境または特定の識別子を持つ環境は、前記着脱可能なコンテンツ蓄積媒体を着脱することのできる特定の機器であるようにした。

本発明のコンテンツ処理方法は、上記方法において、前記特定の環境または特定の識別子を持つ環境は、特定のサービスと契約したことを示す識別子によって特定される環境であるようにした。

- 以上の方法によれば、コンテンツ蓄積媒体に格納された複数の暗号化コンテンツの判別を、当該暗号化コンテンツに関連付けられた情報に基づいて、一段と容易に行うようにすることができる。また、コンテンツ蓄積媒体に格納され

ているコンテンツが使用可能であるか否かを判断することが可能となり、正規のデータでないデータを誤って再生してしまうといった不都合を防止することができる。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理方法であって、前記コンテンツ蓄積媒体上に格納された前記デジタル情報のファイルと関連付けて格納された暗号化データを読み出す暗号化データ読み出しステップと、前記読み出された暗号化データを自身の環境の識別子に関連する情報によって復号化し、特定のデータと合致するかどうかを判定する暗号化データ判別ステップと、を具備するようにした。

本発明のコンテンツ処理方法は、上記方法において、前記暗号化データ読み出しステップでは、前記暗号化された特定のデータは、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる、前記コンテンツ蓄積媒体上の認証ファイルシステム内から読み出されるようにした。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理方法であって、前記コンテンツ蓄積媒体上に格納された前記デジタル情報のファイルと関連付けて格納された識別子を読み出し、自身の環境の識別子と合致するかどうかを判定する識別子判別ステップ、を具備するようにした。

本発明のコンテンツ処理方法は、上記方法において、前記識別子判別ステップでは、前記識別子は、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる、前

記コンテンツ蓄積媒体上の認証ファイルシステム内から読み出されるようにした。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用
5 を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理方法であって、前記コンテンツ蓄積媒体上に格納された前記デジタル情報のファイルと関連付けて格納された暗号化識別子を読み出す暗号化識別子読み出しステップと、前記読み出された暗号化識別子を自身の環境の特定の復号化手段によつて復号化し、自身の識別子と合致するかどうかを判定する暗号化識別子判別ス
10 テップと、を具備するようにした。

本発明のコンテンツ処理方法は、上記方法において、前記暗号化識別子読み出しステップでは、前記暗号化識別子は、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセ
15 スが可能となる、前記コンテンツ蓄積媒体上の認証ファイルシステム内から読み出されるようにした。

本発明のコンテンツ処理方法は、上記方法において、前記コンテンツ処理方法は、さらに、前記暗号化識別子を特定の変換式に対応して変換する識別子逆変換ステップを具備し、前記暗号化識別子判別ステップでは、復号化された暗
20 号化識別子は、前記識別子逆変換部で逆変換されてから自身の識別子と合致するか否かが判定されるようにした。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デ
25 ジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理方法であって、前記コンテンツ蓄積媒体上に格納された前記デジタル情報のファイルと関連付けて格納された固有データを読み出す固有データ読み出しステップと、

前記読み出された固有データを自身の環境の固有データと合致するかどうかを判定する固有データ判別ステップと、を具備するようにした。

本発明のコンテンツ処理方法は、上記方法において、前記固有データ読み出しステップでは、前記固有データは、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる、前記コンテンツ蓄積媒体上の認証ファイルシステム内から読み出されるようにした。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理方法であって、前記コンテンツ蓄積媒体上に格納された、前記デジタル情報のファイルと関連付けられた前記デジタル情報の書き込み時刻を読み出す書き込み時刻読み出しステップと、前記読み出された書き込み時刻と、自身の環境に格納されている書き込み時刻のひとつとが合致するか否かを判定する書き込み時刻判別ステップと、を具備するようにした。

本発明のコンテンツ処理方法は、上記方法において、前記書き込み時刻読み出しステップでは、前記書き込み時刻は、前記着脱可能なコンテンツ蓄積媒体と前記特定の環境との間での認証が成功した場合にのみアクセスが可能となる、前記コンテンツ蓄積媒体上の認証ファイルシステム内から読み出されるようにした。

本発明のコンテンツ処理方法は、上記方法において、前記情報管理システムは、特定の識別子を持つ環境でのみ前記デジタル情報の利用を許可するものであって、前記書き込み時刻判別ステップでは、前記書き込み時刻読み出しステップで読み出された書き込み時刻が、自身の環境の持つ識別子に関連する情報を用いて復号されてから自身の環境に格納されている書き込み時刻のひとつと合致するか否か判定されるようにした。

本発明のコンテンツ処理方法は、上記方法において、さらに、前記書き込み時刻読み出しステップで読み出された書き込み時刻を、前記識別子に関連する情報を利用して変換する書き込み時刻変換ステップを具備し、前記書き込み時刻判別ステップでは、前記変換された書き込み時刻が特定の方法で復号されてから自身の環境に格納されている書き込み時刻のひとつと合致するか否かが判定されるようにした。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理方法であって、前記コンテンツ蓄積媒体上に格納された、前記デジタル情報のファイルと関連付けられた、ユーザによって指定されたユーザ指定値を読み出すユーザ指定値読み出しステップと、前記読み出されたユーザ指定値と、自身の環境に格納されているユーザ指定値が合致するか否かを判定するユーザ指定値判別ステップと、を具備するようにした。

本発明のコンテンツ処理方法は、上記方法において、前記情報管理システムは、特定の識別子を持つ環境でのみ前記デジタル情報の利用を許可するものであって、前記ユーザ指定値判別ステップでは、前記ユーザ指定値読み出し部で読み出されたユーザ指定値は、自身の環境の持つ識別子に関連する情報を用いて復号されてから自身の環境に格納されているユーザ指定値と合致するか否かが判定されるようにした。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理方法であって、前記コンテンツ蓄積媒体上に格納された、前記デジタル情報のファイルと関連付けられた特定のデータを読み出す書き込み特定データ読み出しステップと、前記読み

出された特定のデータと、自身の環境に格納されている特定のデータのひとつと合致するか否かを判定する書き込み特定データ判別ステップと、を具備するようにした。

本発明のコンテンツ処理方法は、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理方法であって、前記コンテンツ蓄積媒体上に格納された、前記デジタル情報のファイルの格納箇所である書き込み箇所を前記コンテンツ蓄積媒体上から読み出す書き込み箇所読み出しステップと、前記読み出された書き込み箇所と、自身の環境に格納されている書き込み箇所のひとつと合致するか否かを判定する書き込み箇所判別ステップと、を具備するようにした。

本発明のコンテンツ処理方法は、上記方法において、前記特定の環境または特定の識別子を持つ環境は、前記着脱可能なコンテンツ蓄積媒体を着脱することのできる特定の機器であるようにした。

本発明のコンテンツ処理方法は、上記方法において、前記特定の環境または特定の識別子を持つ環境は、特定のサービスと契約したことを示す識別子によって特定される環境であるようにした。

以上の方法によれば、コンテンツ蓄積媒体に格納された暗号化コンテンツを読み出し、復号化する前に、当該暗号化コンテンツに関連付けられた情報を基に、暗号化コンテンツを判別することにより、暗号化コンテンツを復号化することなく、その内容を容易に判別することができる。また、コンテンツ蓄積媒体に格納されているコンテンツが使用可能であるか否かを判断することが可能となり、正規のデータでないデータを誤って再生してしまうといった不都合を防止することができる。

本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報

の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報の前記コンテンツ蓄積媒体への書き込みを行うコンテンツ処理プログラムであって、前記識別子に関連する情報を暗号化の鍵として特定のデータを暗号化するデータ暗号化ステップと、前記暗号化された

5 特定のデータを前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する暗号化データ格納ステップと、を具備するようにした。

本発明のコンテンツ処理プログラムは、前記暗号化データ格納ステップでは、前記暗号化された特定のデータの前記コンテンツ蓄積媒体上の格納先として、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間で

10 の認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納されるとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された特定のデータとの関連付けが行なわれるようにした。

本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報

15 の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報の前記コンテンツ蓄積媒体への書き込みを行うコンテンツ処理プログラムであって、前記識別子を前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する識別子格納ステップを具備するようにした。

20 本発明のコンテンツ処理プログラムは、前記識別子格納ステップでは、前記識別子の前記コンテンツ蓄積媒体上の格納先として、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納されるとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された識別

25 子との関連付けが行なわれるようにした。

本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報

の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記蓄積媒体に書き込むコンテンツ処理プログラムであって、特定の暗号化手段を用いて前記識別子を暗号化する識別子暗号化ステップと、前記暗号化された識別子を前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する暗号化識別子格納ステップと、を備えるようにした。

本発明のコンテンツ処理プログラムは、前記暗号化識別子格納ステップでは、前記暗号化識別子の前記コンテンツ蓄積媒体上の格納先として、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納されるとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された暗号化識別子との関連付けが行なわれるようにした。

本発明のコンテンツ処理プログラムは、前記コンテンツ処理方法は、さらに、前記識別子を特定の変換式に対応して変換する識別子変換ステップを具備し、前記識別子暗号化ステップでは、前記識別子変換ステップによって変換された識別子が暗号化され、前記暗号化識別子格納ステップでは、当該暗号化された識別子が前記コンテンツ蓄積媒体に格納されるようにした。

本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理プログラムであって、前記識別子とは異なる、前記特定の識別子を持つ環境に固有な特定のデータを、前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する固有データ格納ステップを備えるようにした。

本発明のコンテンツ処理プログラムは、前記固有データ格納ステップでは、前記特定のデータの前記コンテンツ蓄積媒体上の格納先として、前記着脱可能

なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納されるとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された前記特定のデータとの関連付けが行なわれるようにした。

- 5 本発明のコンテンツ処理プログラムは、デジタル情報を着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムに用いられる、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理プログラムであって、前記デジタル情報を前記コンテンツ蓄積媒体に書き込んだ時刻を特定する書き込み時刻特定ステップと、前記特定された時刻を、書き込みを行なう自身の環境に格納するとともに、前記デジタル情報のファイルと関連付けた上で前記コンテンツ蓄積媒体に格納する書き込み時刻格納ステップと、を具備するようにした。

- 15 本発明のコンテンツ処理プログラムは、前記書き込み時刻格納ステップでは、前記書き込み時刻の前記コンテンツ蓄積媒体上の格納先として、前記着脱可能なコンテンツ蓄積媒体と前記特定の環境との間での認証が成功した場合にのみアクセスが可能となる認証ファイルシステム内に格納されるとともに、前記デジタル情報のファイルと前記認証ファイルシステム内に格納された前記書き込み時刻との関連付けが行なわれるようにした。

- 20 本発明のコンテンツ処理プログラムは、前記情報管理システムは、特定の識別子を持つ環境でのみ前記デジタル情報の利用を許可するものであって、前記コンテンツ処理プログラムは、さらに、前記書き込み時刻を前記識別子に関連する情報を用いて暗号化する書き込み時刻暗号化ステップを備え、前記書き込み時刻格納ステップでは、少なくともコンテンツ蓄積媒体に格納する書き込み時刻が、前記書き込み時刻暗号化部によって暗号化されたものとなるようにした。

- 25 た。
- 本発明のコンテンツ処理プログラムは、さらに、前記識別子に関連する情報を利用して前記書き込み時刻を変換する書き込み時刻変換ステップを具備し、

前記書き込み時刻暗号化ステップでは、前記変換された書き込み時刻が特定の
方法で暗号化されるようにした。

- 本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを
着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報
5 の利用を特定の環境でのみ許可する情報管理システムにおいて用いられる、前
記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理プログ
ラムであって、ユーザが指定する値あるいは名称であるユーザ指定値を環境に
設定するユーザ指定値書き込みステップと、前記ユーザ指定値を前記コンテ
ンツ蓄積媒体に格納するユーザ指定値格納ステップと、を具備するようにした。
- 10 本発明のコンテンツ処理プログラムは、さらに、ユーザがユーザ指定値を指
定していない状態でユーザ指定値として利用するための初期値をランダムに
設定する、初期値設定ステップを具備するようにした。

- 本発明のコンテンツ処理プログラムは、前記情報管理システムは、特定の識
別子を持つ環境でのみ前記デジタル情報の利用を許可するものであって、前記
15 コンテンツ処理プログラムは、さらに、前記ユーザ指定値を前記識別子に関連
する情報を用いて暗号化するユーザ指定値暗号化ステップを具備し、前記ユー
ザ指定値格納ステップでは、前記コンテンツ蓄積媒体に格納するユーザ指定値
が、前記ユーザ指定値暗号化部によって暗号化されたものとなるようにした。

- 本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを
20 着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報
の利用を特定の環境でのみ許可する情報管理システムにおいて用いられる、前
記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理プログ
ラムであって、前記デジタル情報を前記コンテンツ蓄積媒体に書き込む際に特
定のデータを作成する書き込み特定データ生成ステップと、前記特定のデー
25 を、書き込みを行なう自身の環境に格納するとともに、前記デジタル情報のフ
ァイルと関連付けた上で前記コンテンツ蓄積媒体に格納する書き込み特定デ
ータ格納ステップと、を具備するようにした。

本発明のコンテンツ処理プログラムは、前記書き込み特定データ生成ステップにおいて、前記特定のデータは、書き込みの際にランダムに生成されるか、あるいは特定の手順によって生成されるようにした。

- 本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを
- 5 着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理プログラムであって、前記デジタル情報を前記コンテンツ蓄積媒体に書き込んだ際の書き込み箇所を特定する書き込み箇所特定ステップと、前記特定された箇所を、
- 10 書き込みを行なう自身の環境に格納する書き込み箇所格納ステップと、を具備するようにした。

本発明のコンテンツ処理プログラムは、前記デジタル情報は、前記識別子に関連する情報を利用して暗号化されているようにした。

- 本発明のコンテンツ処理プログラムは、前記特定のデータは、なんらかの意味を持つ文字列、数値、画像、音声等のデータであるようにした。
- 15

本発明のコンテンツ処理プログラムは、前記識別子は、なんらかの意味を持つ文字列、数値、画像、音声等のデータであるようにした。

- 本発明のコンテンツ処理プログラムは、前記特定の環境または特定の識別子を持つ環境は、前記着脱可能なコンテンツ蓄積媒体を着脱することのできる特定の機器であるようにした。
- 20

本発明のコンテンツ処理プログラムは、前記特定の環境または特定の識別子を持つ環境は、特定のサービスと契約したことを示す識別子によって特定される環境であるようにした。

- 以上の構成によれば、コンテンツ蓄積媒体に格納された複数の暗号化コンテンツの判別を、当該暗号化コンテンツに関連付けられた情報に基づいて、一段と容易に行うようにすることができる。また、コンテンツ蓄積媒体に格納されているコンテンツが使用可能であるか否かを判断することが可能となり、正規
- 25

のデータでないデータを誤って再生してしまうといった不都合を防止することができる。

本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報
5 の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理プログラムであって、前記コンテンツ蓄積媒体上に格納された前記デジタル情報のファイルと関連付けて格納された暗号化データを読み出す暗号化データ読み出しステップと、前記読み出された暗号化データを自身の環境の
10 識別子に関連する情報によって復号化し、特定のデータと合致するかどうかを判定する暗号化データ判別ステップと、を具備するようにした。

本発明のコンテンツ処理プログラムは、前記暗号化データ読み出しステップでは、前記暗号化された特定のデータは、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる、前記コンテンツ蓄積媒体上の認証ファイルシステム内から読み出されるようにした。

本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて
20 用いられる、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理プログラムであって、前記コンテンツ蓄積媒体上に格納された前記デジタル情報のファイルと関連付けて格納された識別子を読み出し、自身の環境の識別子と合致するかどうかを判定する識別子判別ステップ、を具備するようにした。

25 本発明のコンテンツ処理プログラムは、前記識別子判別ステップでは、前記識別子は、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる、前記コンテンツ

蓄積媒体上の認証ファイルシステム内から読み出されるようにした。

- 本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて
- 5 用いられる、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理プログラムであって、前記コンテンツ蓄積媒体上に格納された前記デジタル情報のファイルと関連付けて格納された暗号化識別子を読み出す暗号化識別子読み出しステップと、前記読み出された暗号化識別子を自身の環境の特定の復号化手段によって復号化し、自身の識別子と合致するかどうかを判定
- 10 する暗号化識別子判別ステップと、を具備するようにした。

- 本発明のコンテンツ処理プログラムは、前記暗号化識別子読み出しステップでは、前記暗号化識別子は、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる、前記コンテンツ蓄積媒体上の認証ファイルシステム内から読み出されるよ
- 15 うにした。

- 本発明のコンテンツ処理プログラムは、さらに、前記暗号化識別子を特定の変換式に対応して変換する識別子逆変換ステップを具備し、前記暗号化識別子判別ステップでは、復号化された暗号化識別子は、前記識別子逆変換部で逆変換されてから自身の識別子と合致するか否かが判定されるようにした。

- 20 本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理プログラムであって、前記コンテンツ蓄積媒体上に格納された前記デ
- 25 ジタル情報のファイルと関連付けて格納された固有データを読み出す固有データ読み出しステップと、前記読み出された固有データを自身の環境の固有データと合致するかどうかを判定する固有データ判別ステップと、を具備するよ

うにした。

本発明のコンテンツ処理プログラムは、前記固有データ読み出しステップでは、前記固有データは、前記着脱可能なコンテンツ蓄積媒体と前記特定の識別子を持つ環境との間での認証が成功した場合にのみアクセスが可能となる、前記コンテンツ蓄積媒体上の認証ファイルシステム内から読み出されるようにした。

本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理プログラムであって、前記コンテンツ蓄積媒体上に格納された、前記デジタル情報のファイルと関連付けられた前記デジタル情報の書き込み時刻を読み出す書き込み時刻読み出しステップと、前記読み出された書き込み時刻と、自身の環境に格納されている書き込み時刻のひとつとが合致するか否かを判定する書き込み時刻判別ステップと、を具備するようにした。

本発明のコンテンツ処理プログラムは、前記書き込み時刻読み出しステップでは、前記書き込み時刻は、前記着脱可能なコンテンツ蓄積媒体と前記特定の環境との間での認証が成功した場合にのみアクセスが可能となる、前記コンテンツ蓄積媒体上の認証ファイルシステム内から読み出されるようにした。

本発明のコンテンツ処理プログラムは、前記情報管理システムは、特定の識別子を持つ環境でのみ前記デジタル情報の利用を許可するものであって、前記書き込み時刻判別ステップでは、前記書き込み時刻読み出しステップで読み出された書き込み時刻が、自身の環境の持つ識別子に関連する情報を用いて復号されてから自身の環境に格納されている書き込み時刻のひとつと合致するか否かを判定されるようにした。

本発明のコンテンツ処理プログラムは、さらに、前記書き込み時刻読み出しステップで読み出された書き込み時刻を、前記識別子に関連する情報を利用し

て変換する書き込み時刻変換ステップを具備し、前記書き込み時刻判別ステップでは、前記変換された書き込み時刻が特定の 방법으로復号されてから自身の環境に格納されている書き込み時刻のひとつと合致するか否かが判定されるようにした。

- 5 本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理プログラムであって、前記コンテンツ蓄積媒体上に格納された、前記デジタル情報
- 10 のファイルと関連付けられた、ユーザによって指定されたユーザ指定値を読み出すユーザ指定値読み出しステップと、前記読み出されたユーザ指定値と、自身の環境に格納されているユーザ指定値が合致するか否かを判定するユーザ指定値判別ステップと、を具備するようにした。

- 本発明のコンテンツ処理プログラムは、前記情報管理システムは、特定の識別子を持つ環境でのみ前記デジタル情報の利用を許可するものであって、前記
- 15 ユーザ指定値判別ステップでは、前記ユーザ指定値読み出し部で読み出されたユーザ指定値は、自身の環境の持つ識別子に関連する情報を用いて復号されてから自身の環境に格納されているユーザ指定値と合致するか否かが判定されるようにした。

- 20 本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理プログラムであって、前記コンテンツ蓄積媒体上に格納された、前記デジタル情報
- 25 のファイルと関連付けられた特定のデータを読み出す書き込み特定データ読み出しステップと、前記読み出された特定のデータと、自身の環境に格納されている特定のデータのひとつと合致するか否かを判定する書き込み特定デー

タ判別ステップと、を具備するようにした。

- 本発明のコンテンツ処理プログラムは、デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の環境でのみ許可する情報管理システムにおいて用いられる、前
- 5 記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理プログラムであって、前記コンテンツ蓄積媒体上に格納された、前記デジタル情報のファイルの格納箇所である書き込み箇所を前記コンテンツ蓄積媒体上から読み出す書き込み箇所読み出しステップと、前記読み出された書き込み箇所と、自身の環境に格納されている書き込み箇所のひとつと合致するか否かを判定
- 10 する書き込み箇所判別ステップと、を具備するようにした。

本発明のコンテンツ処理プログラムは、前記特定の環境または特定の識別子を持つ環境は、前記着脱可能なコンテンツ蓄積媒体を着脱することのできる特定の機器であるようにした。

- 本発明のコンテンツ処理プログラムは、前記特定の環境または特定の識別子
- 15 を持つ環境は、特定のサービスと契約したことを示す識別子によって特定される環境であるようにした。

- 以上の構成によれば、コンテンツ蓄積媒体に格納された暗号化コンテンツを読み出し、復号化する前に、当該暗号化コンテンツに関連付けられた情報を基に、暗号化コンテンツを判別することにより、暗号化コンテンツを復号化する
- 20 ことなく、その内容を容易に判別することができる。また、コンテンツ蓄積媒体に格納されているコンテンツが使用可能であるか否かを判断することが可能となり、正規のデータでないデータを誤って再生してしまうといった不都合を防止することができる。

- 本明細書は、2002年3月29日出願の特願2002-097429に基づ
- 25 づくものである。この内容をここに含めておく。

産業上の利用可能性

本発明は、例えばコンテンツ蓄積媒体を着脱可能な携帯端末装置に用いるに好適である。

請 求 の 範 囲

1. デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報の前記コンテンツ蓄積媒体への書き込みを行うコンテンツ処理装置であって、
 - 5 前記識別子又は前記識別子に関連する情報を暗号化の鍵として特定のデータを暗号化するデータ暗号化部と、
前記暗号化された特定のデータを前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する暗号化データ格納部と、
 - 10 を具備するコンテンツ処理装置。
 2. デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記蓄積媒体に書き込むコンテンツ処理装置であって、
 - 15 特定の暗号化手段を用いて前記識別子又は前記識別子に関連する情報を暗号化する識別子暗号化部と、
前記暗号化された識別子又は前記暗号化された関連する情報を前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する暗号化識別子格納部と、
 - 20 を具備するコンテンツ処理装置。
 3. デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むコンテンツ処理装置であって、
 - 25 前記特定の識別子とは異なる、前記特定の識別子を持つ環境に固有な特定のデータを、前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する固有データ格納部を具備するコンテンツ処理装置。

4. 前記環境に固有な特定のデータは、ユーザが指定する値又は名称である請求の範囲3記載のコンテンツ処理装置。

5. 前記コンテンツ処理装置は、さらに、ユーザが前記値又は名称を指定していない状態でその値又は名称として利用するための初期値をランダムに設定

5 する初期値設定部を具備する請求の範囲4記載のコンテンツ処理装置。

6. 前記コンテンツ処理装置は、さらに、前記値又は名称を前記識別子に関連する情報を用いて暗号化するユーザ指定値暗号化部を具備し、

前記固有データ格納部は、前記コンテンツ蓄積媒体に格納する値又は名称を、前記ユーザ指定値暗号化部によって暗号化されたものとする請求の範囲5記

10 載のコンテンツ処理装置。

7. 前記特定の識別子を持つ環境は、特定のサービスと契約したことを示す前記識別子によって特定される環境である請求の範囲1から6のいずれかに記載のコンテンツ処理装置。

8. デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理装置であって、

前記コンテンツ蓄積媒体上に前記デジタル情報のファイルと関連付けて格納された暗号化データを読み出す暗号化データ読み出し部と、

20 前記読み出された暗号化データを自身の環境の前記識別子又は自身の環境の前記識別子に関連する情報によって復号化し、特定のデータと合致するか否かを判定する暗号化データ判別部と、

を具備するコンテンツ処理装置。

9. デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理装置であって、

前記コンテンツ蓄積媒体上に前記デジタル情報のファイルと関連付けて格納された、前記識別子が暗号化されてなる暗号化識別子又は前記識別子に関連する情報が暗号化されてなる暗号化情報を読み出す暗号化識別子読み出し部と、

- 5 前記読み出された暗号化識別子又は暗号化情報を自身の環境の特定の復号化手段によって復号化し、自身の識別子又は識別子に関連する情報と合致するか否かを判定する暗号化識別子判別部と、

を具備するコンテンツ処理装置。

- 10 10. デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理装置であって、

前記コンテンツ蓄積媒体上に前記デジタル情報のファイルと関連付けて格納された固有データを読み出す固有データ読み出し部と、

- 15 前記読み出された固有データが自身の環境に固有な特定のデータと合致するか否かを判定する固有データ判別部と、

を具備するコンテンツ処理装置。

- 20 11. 前記環境に固有な特定のデータは、ユーザによって指定されたユーザ指定値であり、前記固有データ判別部は、前記コンテンツ蓄積媒体から読み出された前記固有データと自身の環境に格納されている前記ユーザ指定値とが合致するか否かを判定する請求の範囲10記載のコンテンツ処理装置。

- 25 12. 前記固有データ判別部は、前記読み出された固有データを、自身の環境の持つ前記識別子に関連する情報を用いて復号した後、当該復号された固有データが自身の環境に格納されている前記ユーザ指定値と合致するか否かを判定する請求の範囲11記載のコンテンツ処理装置。

13. 前記特定の識別子を持つ環境は、特定のサービスと契約したことを示す前記識別子によって特定される環境である請求の範囲8から12のいずれか

に記載のコンテンツ処理装置。

1 4. デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上の
ファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境で
のみ許可する情報管理システムにおいて用いられる前記コンテンツ蓄積媒体

5 であって、

前記識別子又は前記識別子に関連する情報を暗号化の鍵として暗号化され
た特定のデータが、前記デジタル情報のファイルと関連付けられて格納されて
いるコンテンツ蓄積媒体。

1 5. デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上の
10 ファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境で
のみ許可する情報管理システムにおいて用いられる前記コンテンツ蓄積媒体
であって、

前記識別子が特定の暗号化手段によって暗号化されてなる暗号化識別子又は
は前記識別子に関連する情報が特定の暗号化手段によって暗号化されてなる
15 暗号化情報が、前記デジタル情報のファイルと関連付けて格納されているコン
テンツ蓄積媒体。

1 6. デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上の
ファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境で
のみ許可する情報管理システムにおいて用いられる前記コンテンツ蓄積媒体
20 であって、

前記特定の識別子とは異なる、前記特定の識別子を持つ環境に固有な特定の
データが、前記デジタル情報のファイルと関連付けられて格納されているコン
テンツ蓄積媒体。

1 7. 前記環境に固有な特定のデータは、ユーザが指定した値又は名称である
25 請求の範囲 1 6 記載のコンテンツ蓄積媒体。

1 8. 前記ユーザが指定した値又は名称としては、ユーザがその値又は名称を
指定していない状態では、初期値としてランダムな値が格納されている請求の

範囲 1 7 記載のコンテンツ蓄積媒体。

1 9. 前記値又は名称は前記識別子に関連する情報を用いて暗号化されて格納されている請求の範囲 1 7 記載のコンテンツ蓄積媒体。

2 0. 前記識別子は、特定のサービスと契約したことを示すデータである請求
5 の範囲 1 4 から 1 9 のいずれかに記載のコンテンツ蓄積媒体。

2 1. デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上の
ファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境で
のみ許可する情報管理システムにおいて、前記デジタル情報の前記コンテンツ
蓄積媒体への書き込みを行うコンテンツ処理方法であって、

10 前記識別子又は前記識別子に関連する情報を暗号化の鍵として特定のデー
タを暗号化するデータ暗号化ステップと、

前記暗号化された特定のデータを前記デジタル情報のファイルと関連付け
て前記コンテンツ蓄積媒体上に格納する暗号化データ格納ステップと、
を具備するコンテンツ処理方法。

15 2 2. デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上の
ファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境で
のみ許可する情報管理システムにおいて、前記デジタル情報を前記蓄積媒体に
書き込むコンテンツ処理方法であって、

特定の暗号化手段を用いて前記識別子又は前記識別子に関連する情報を暗
20 号化する識別子暗号化ステップと、

前記暗号化された識別子又は前記暗号化された関連する情報を前記デジ
タル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する暗号化
識別子格納ステップと、

を備えるコンテンツ処理方法。

25 2 3. デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上の
ファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境で
のみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ

蓄積媒体に書き込むコンテンツ処理方法であって、

前記特定の識別子とは異なる、前記特定の識別子を持つ環境に固有な特定のデータを、前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する固有データ格納ステップを備えるコンテンツ処理方法。

- 5 24. 前記環境に固有な特定のデータは、ユーザが指定する値又は名称である請求の範囲23記載のコンテンツ処理方法。

25. 前記コンテンツ処理方法は、さらに、ユーザが前記値又は名称を指定していない状態でその値又は名称として利用するための初期値をランダムに設定する初期値設定ステップを具備する請求の範囲24記載のコンテンツ処理
10 方法。

26. 前記コンテンツ処理方法は、さらに、前記値又は名称を前記識別子に関連する情報を用いて暗号化するユーザ指定値暗号化ステップを具備し、

前記固有データ格納ステップでは、前記コンテンツ蓄積媒体に格納する値又は名称が、前記ユーザ指定値暗号化ステップにおいて暗号化されたものとなる

- 15 請求の範囲24記載のコンテンツ処理方法。

27. 前記特定の識別子を持つ環境は、特定のサービスと契約したことを示す識別子によって特定される環境である請求の範囲21から26のいずれかに記載のコンテンツ処理方法。

28. デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上の
20 ファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理方法であって、

前記コンテンツ蓄積媒体上に前記デジタル情報のファイルと関連付けて格納された暗号化データを読み出す暗号化データ読み出しステップと、

- 25 前記読み出された暗号化データを自身の環境の前記識別子又は自身の環境の前記識別子に関連する情報によって復号化し、特定のデータと合致するか否かを判定する暗号化データ判別ステップと、

を具備するコンテンツ処理方法。

29. デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ

- 5 蓄積媒体から読み出すコンテンツ処理方法であって、

前記コンテンツ蓄積媒体上に前記デジタル情報のファイルと関連付けて格納された、前記識別子が暗号化されてなる暗号化識別子又は前記識別子に関連する情報が暗号化されてなる暗号化情報を読み出す暗号化識別子読み出しステップと、

- 10 前記読み出された暗号化識別子又は暗号化情報を自身の環境の特定の復号化手段によって復号化し、自身の識別子又は識別子に関連する情報と合致するか否かを判定する暗号化識別子判別ステップと、

を具備するコンテンツ処理方法。

30. デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上の
15 ファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すコンテンツ処理方法であって、

前記コンテンツ蓄積媒体上に前記デジタル情報のファイルと関連付けて格納された固有データを読み出す固有データ読み出しステップと、

- 20 前記読み出された固有データが自身の環境に固有な特定のデータと合致するか否かを判定する固有データ判別ステップと、

を具備するコンテンツ処理方法。

31. 前記環境に固有な特定のデータは、ユーザによって指定されたユーザ指定値であり、前記固有データ判別ステップでは、前記コンテンツ蓄積媒体から

- 25 読み出された前記固有データと自身の環境に格納されている前記ユーザ指定値とが合致するか否かが判定される請求の範囲30記載のコンテンツ処理方法。

3 2. 前記固有データ判別ステップでは、前記読み出した固有データを、読み出し先の環境が持つ前記識別子に関連する情報を用いて復号した後、当該復号された固有データが読み出し先の環境に格納されている前記ユーザ指定値と合致するか否か判定する請求の範囲 3 1 記載のコンテンツ処理方法。

- 5 3 3. 前記特定の識別子を持つ環境は、特定のサービスと契約したことを示す前記識別子によって特定される環境である請求の範囲 2 8 から 3 2 のいずれかに記載のコンテンツ処理方法。

- 3 4. デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境で
10 のみ許可する情報管理システムにおいて用いられる、前記デジタル情報の前記コンテンツ蓄積媒体への書き込みを行うためのコンテンツ処理プログラムであって、

前記識別子又は前記識別子に関連する情報を暗号化の鍵として特定のデータを暗号化するデータ暗号化ステップと、

- 15 前記暗号化された特定のデータを前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する暗号化データ格納ステップと、
を具備するコンテンツ処理プログラム。

- 3 5. デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境で
20 のみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記蓄積媒体に書き込むためのコンテンツ処理プログラムであって、

特定の暗号化手段を用いて前記識別子又は前記識別子に関連する情報を暗号化する識別子暗号化ステップと、

- 前記暗号化された識別子又は前記暗号化された関連する情報を前記デジタル
25 情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する暗号化識別子格納ステップと、

を具備するコンテンツ処理プログラム。

36. デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記コンテンツ蓄積媒体に書き込むためのコンテンツ処理プログラムであって、

- 5 前記特定の識別子とは異なる、前記特定の識別子を持つ環境に固有な特定のデータを、前記デジタル情報のファイルと関連付けて前記コンテンツ蓄積媒体上に格納する固有データ格納ステップを具備するコンテンツ処理プログラム。

37. 前記環境に固有な特定のデータは、ユーザが指定する値又は名称である請求の範囲36記載のコンテンツ処理プログラム。

- 10 38. 前記コンテンツ処理プログラムは、さらに、ユーザが前記値又は名称を指定していない状態でその値又は名称として利用するための初期値をランダムに設定する初期値設定ステップを具備する請求の範囲37記載のコンテンツ処理プログラム。

39. 前記コンテンツ処理プログラムは、さらに、前記値又は名称を前記識別

- 15 子に関連する情報を用いて暗号化するユーザ指定値暗号化ステップを具備し、前記固有データ格納ステップでは、前記コンテンツ蓄積媒体に格納する値又は名称が、前記ユーザ指定値暗号化ステップにおいて暗号化されたものとなる請求の範囲37記載のコンテンツ処理プログラム。

40. 前記特定の識別子を持つ環境は、特定のサービスと契約したことを示す

- 20 識別子によって特定される環境である請求の範囲34から39のいずれかに記載のコンテンツ処理プログラム。

41. デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記

- 25 コンテンツ蓄積媒体から読み出すためのコンテンツ処理プログラムであって、

前記コンテンツ蓄積媒体上に前記デジタル情報のファイルと関連付けて格納された暗号化データを読み出す暗号化データ読み出しステップと、

前記読み出された暗号化データを自身の環境の前記識別子又は自身の環境の前記識別子に関連する情報によって復号化し、特定のデータと合致するか否かを判定する暗号化データ判別ステップと、
を具備するコンテンツ処理プログラム。

- 5 4 2. デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記コンテンツ蓄積媒体から読み出すためのコンテンツ処理プログラムであって、
前記コンテンツ蓄積媒体上に前記デジタル情報のファイルと関連付けて格
10 納された、前記識別子が暗号化されてなる暗号化識別子又は前記識別子に関連する情報が暗号化されてなる暗号化情報を読み出す暗号化識別子読み出しステップと、

- 前記読み出された暗号化識別子又は暗号化情報を自身の環境の特定の復号化手段によって復号化し、自身の識別子又は識別子に関連する情報と合致するか否かを判定する暗号化識別子判別ステップと、
15 を具備するコンテンツ処理プログラム。

- 4 3. デジタル情報化されたコンテンツを着脱可能なコンテンツ蓄積媒体上のファイルとして管理し、前記デジタル情報の利用を特定の識別子を持つ環境でのみ許可する情報管理システムにおいて用いられる、前記デジタル情報を前記
20 コンテンツ蓄積媒体から読み出すためのコンテンツ処理プログラムであって、
前記コンテンツ蓄積媒体上に前記デジタル情報のファイルと関連付けて格納された固有データを読み出す固有データ読み出しステップと、

- 前記読み出された固有データが自身の環境に固有な特定のデータと合致するか否かを判定する固有データ判別ステップと、
25 を具備するコンテンツ処理プログラム。

- 4 4. 前記環境に固有な特定のデータは、ユーザによって指定されたユーザ指定値であり、前記固有データ判別ステップでは、前記コンテンツ蓄積媒体から

読み出された前記固有データと自身の環境に格納されている前記ユーザ指定値とが合致するか否かが判定される請求の範囲43記載のコンテンツ処理プログラム。

45. 前記固有データ判別ステップは、前記読み出した固有データを、読み出し先の環境が持つ前記識別子に関連する情報を用いて復号した後、当該復号された固有データが読み出し先の環境に格納されている前記ユーザ指定値と合致するか否かを判定する請求の範囲44記載のコンテンツ処理プログラム。
46. 前記特定の識別子を持つ環境は、特定のサービスと契約したことを示す前記識別子によって特定される環境である請求の範囲41から45のいずれかに記載のコンテンツ処理プログラム。
- 10

1/29

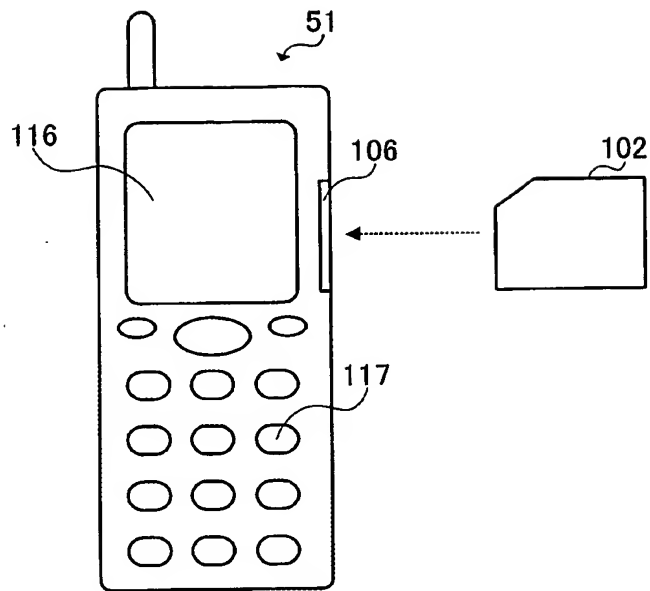


図 1

2/29

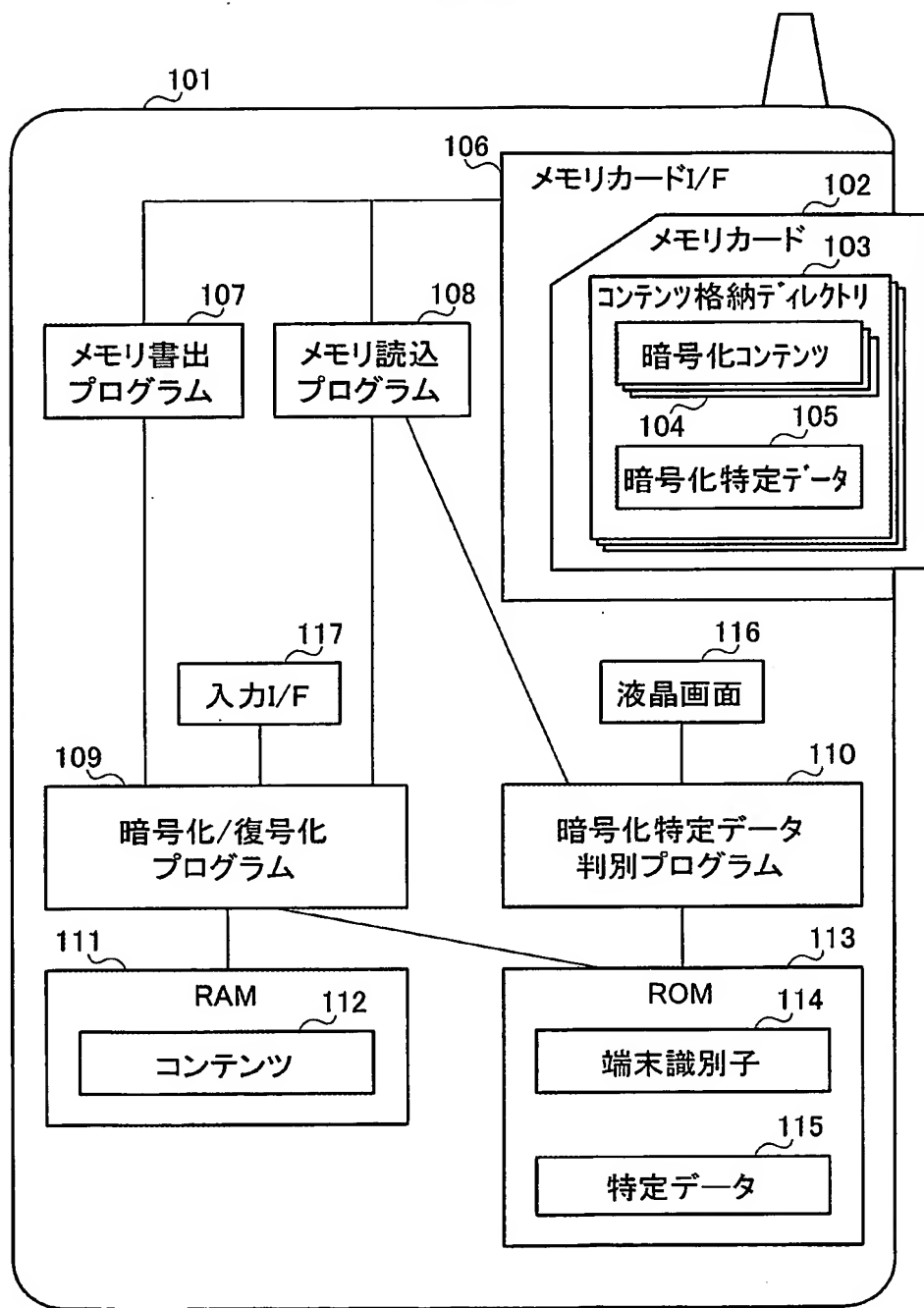


図 2

3/29

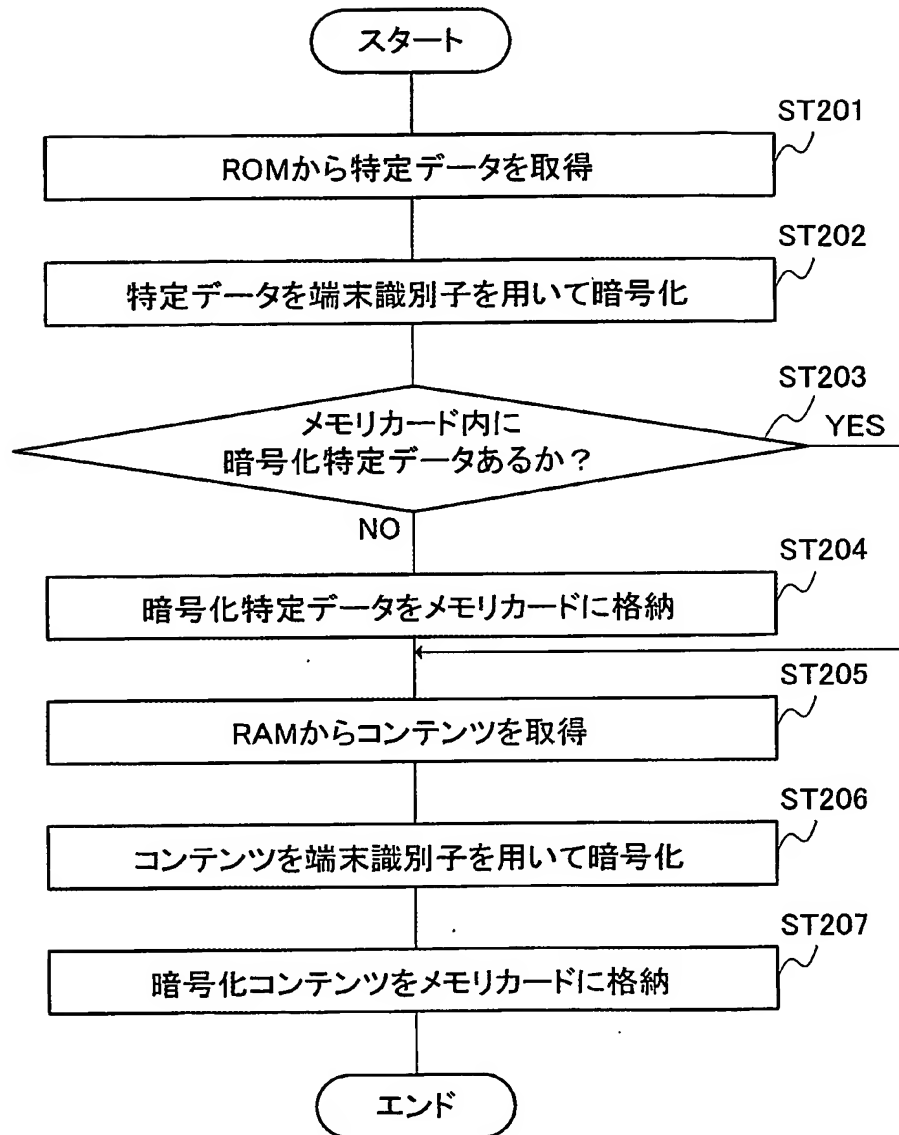


図 3

4/29

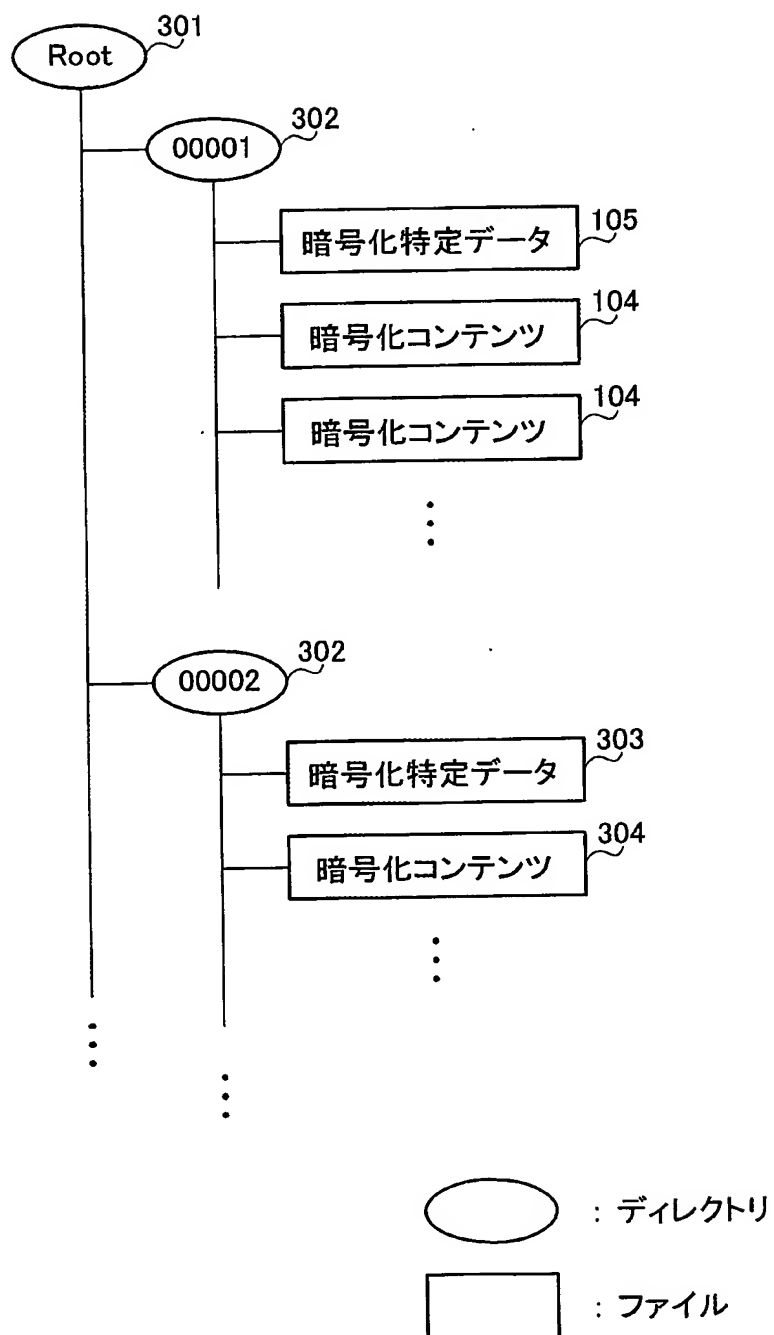


図 4

5/29

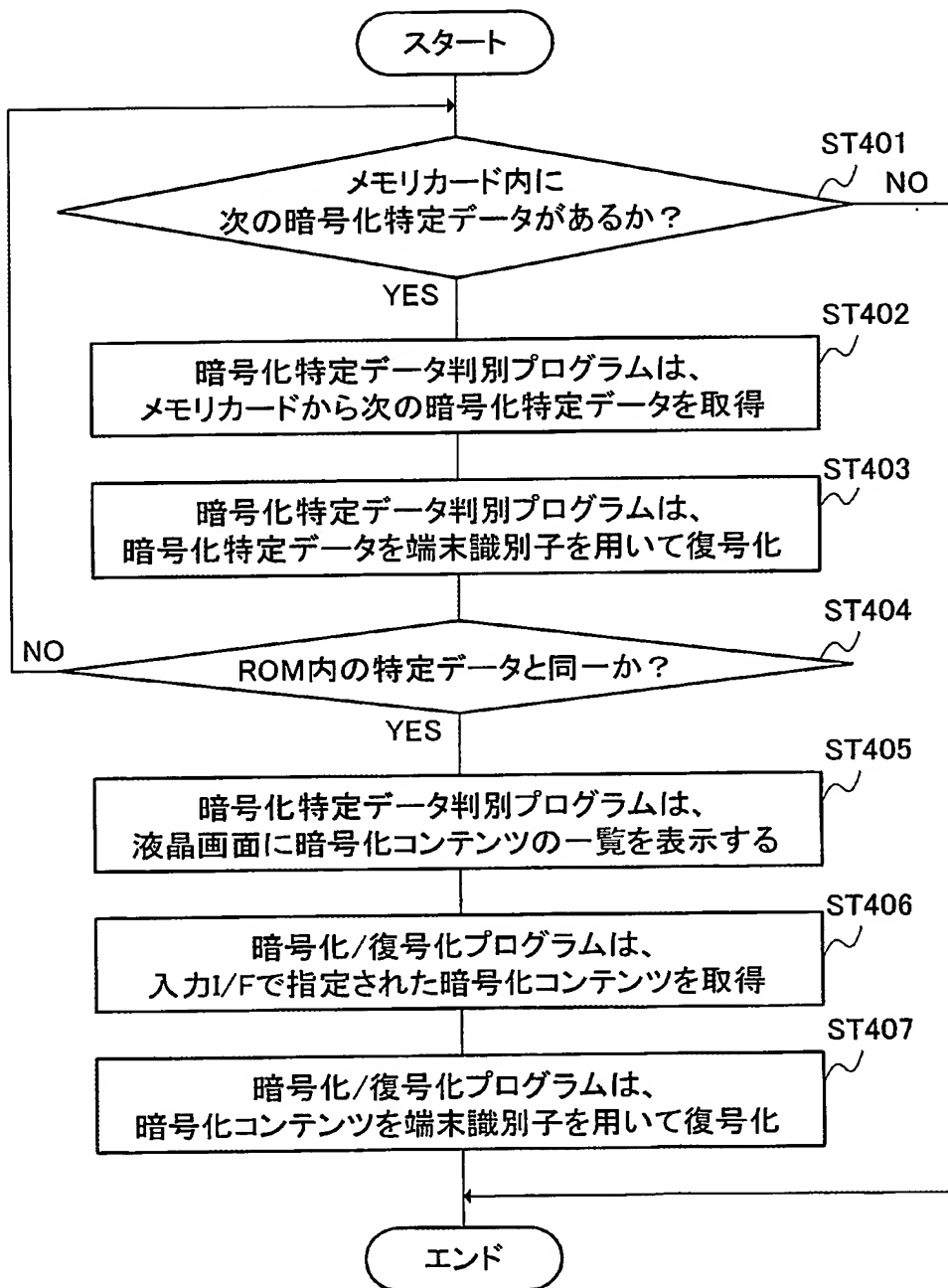


図 5

6/29

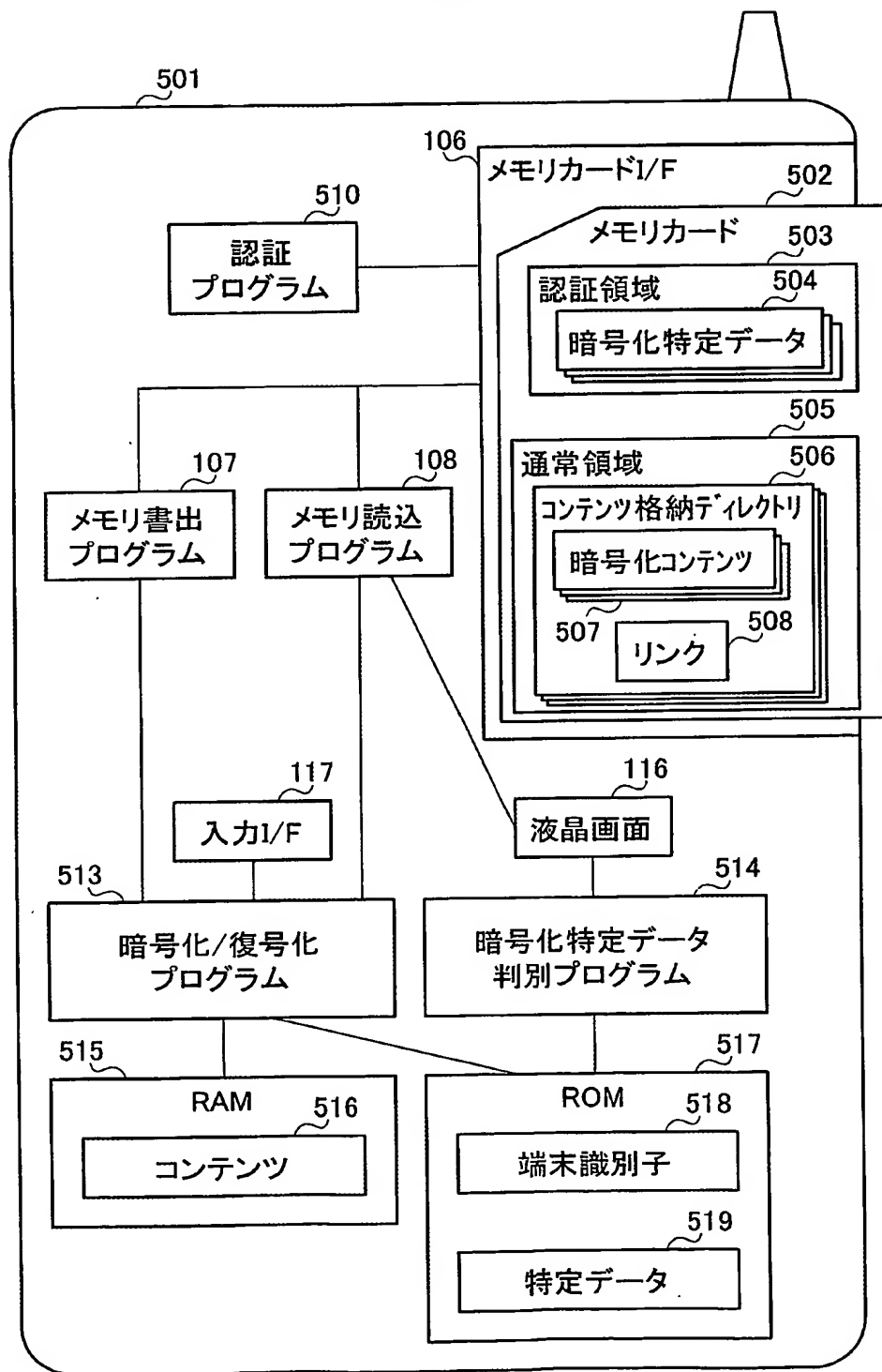


図 6

7/29

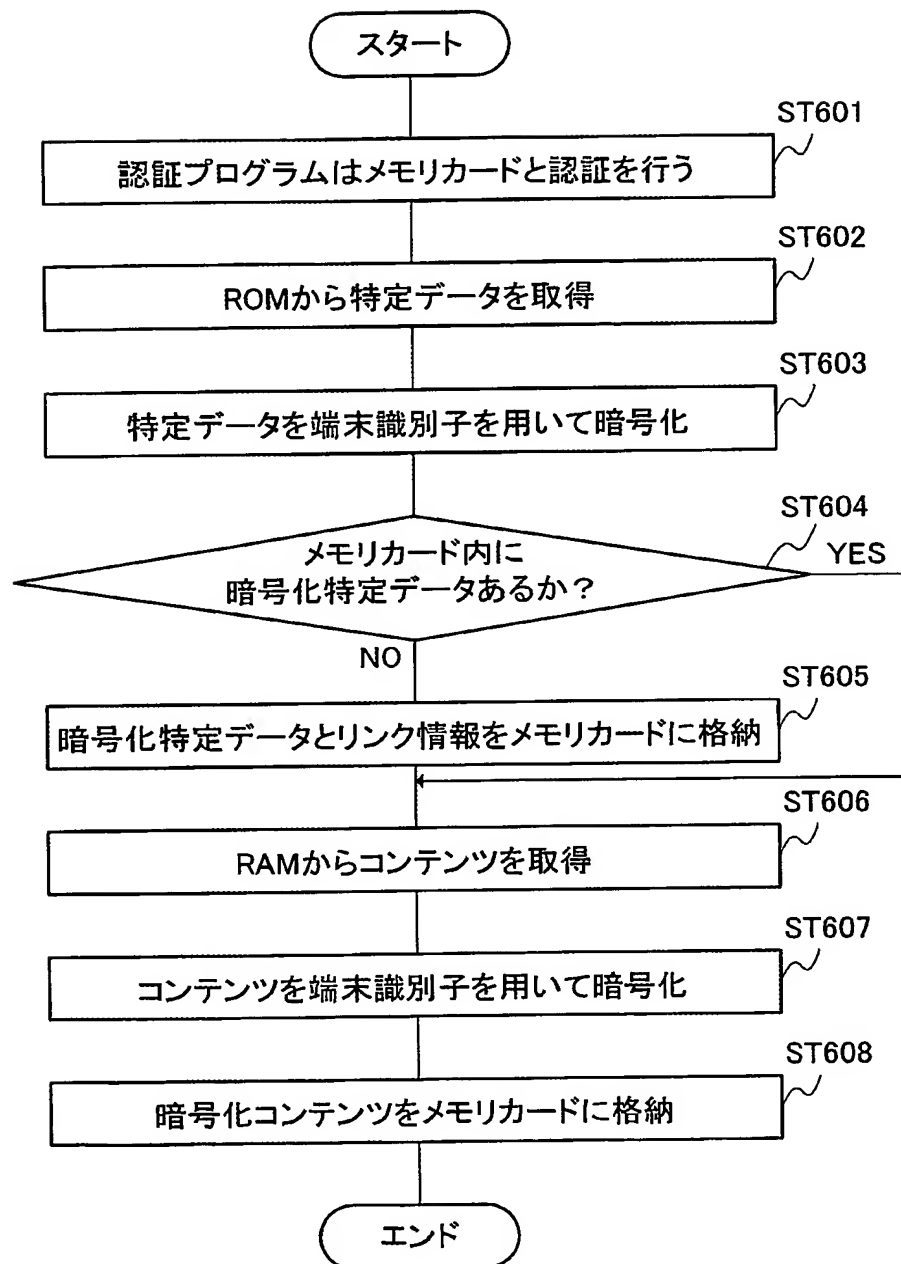


図 7

8/29

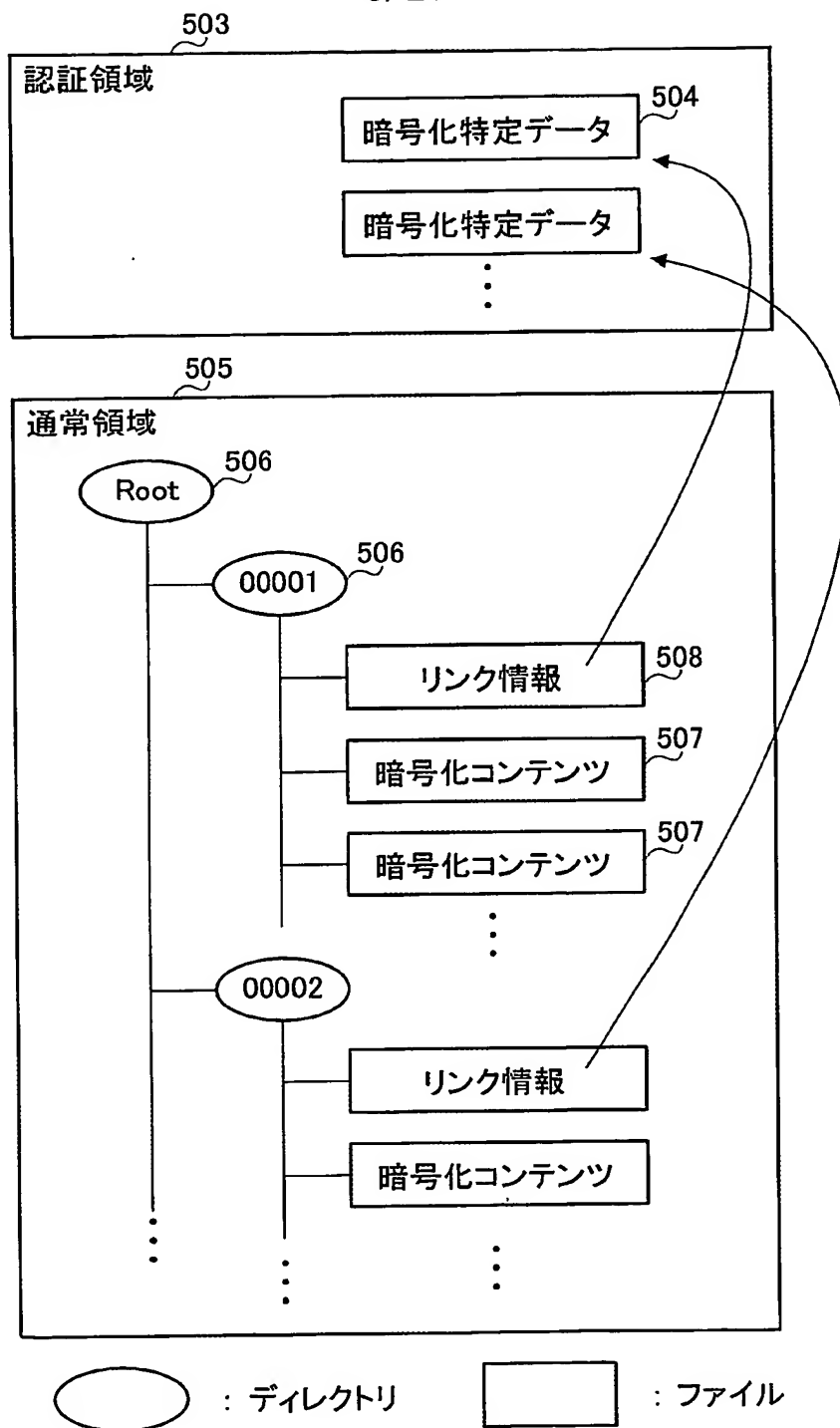


図 8

9/29

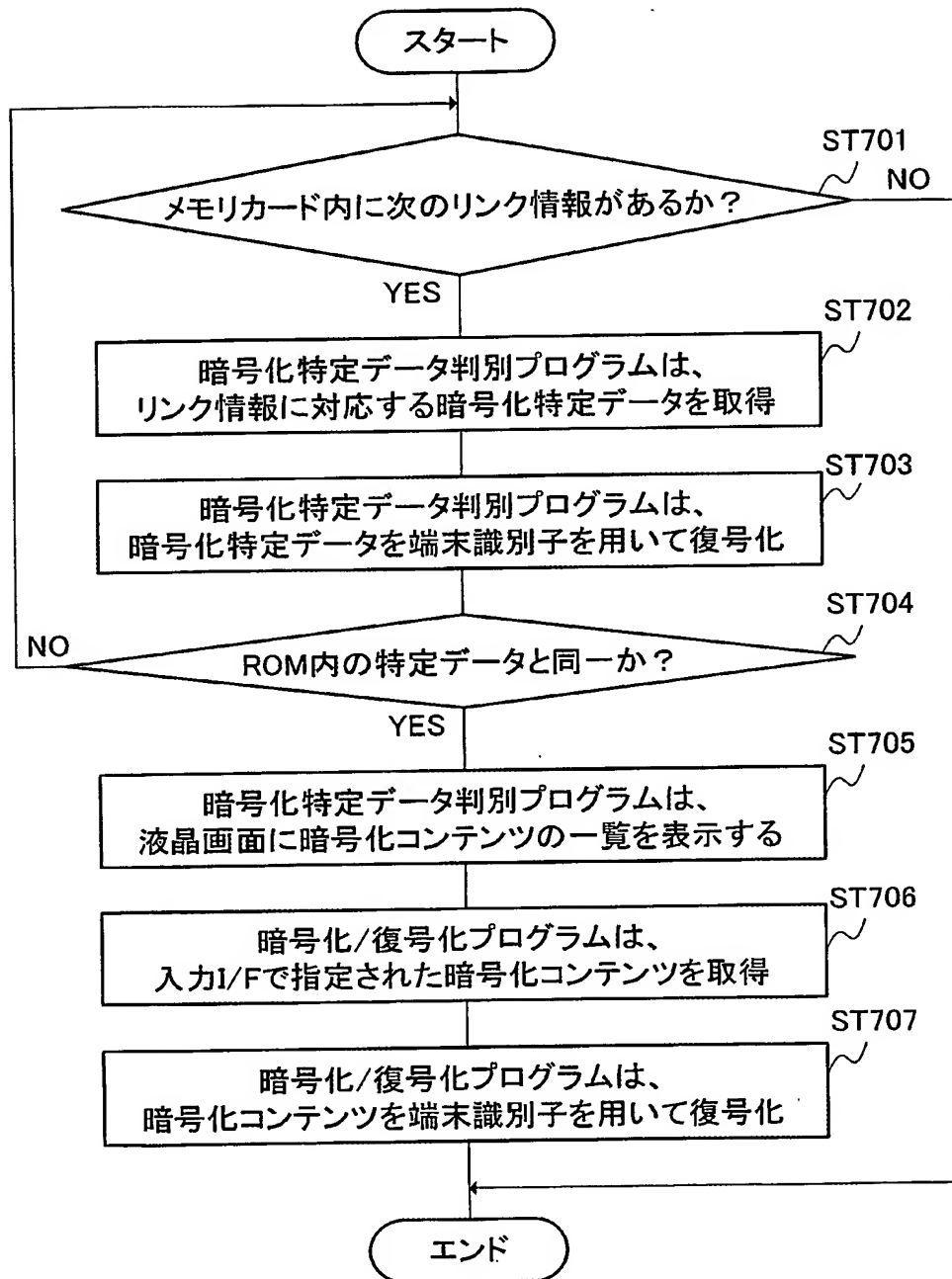


図 9

10/29

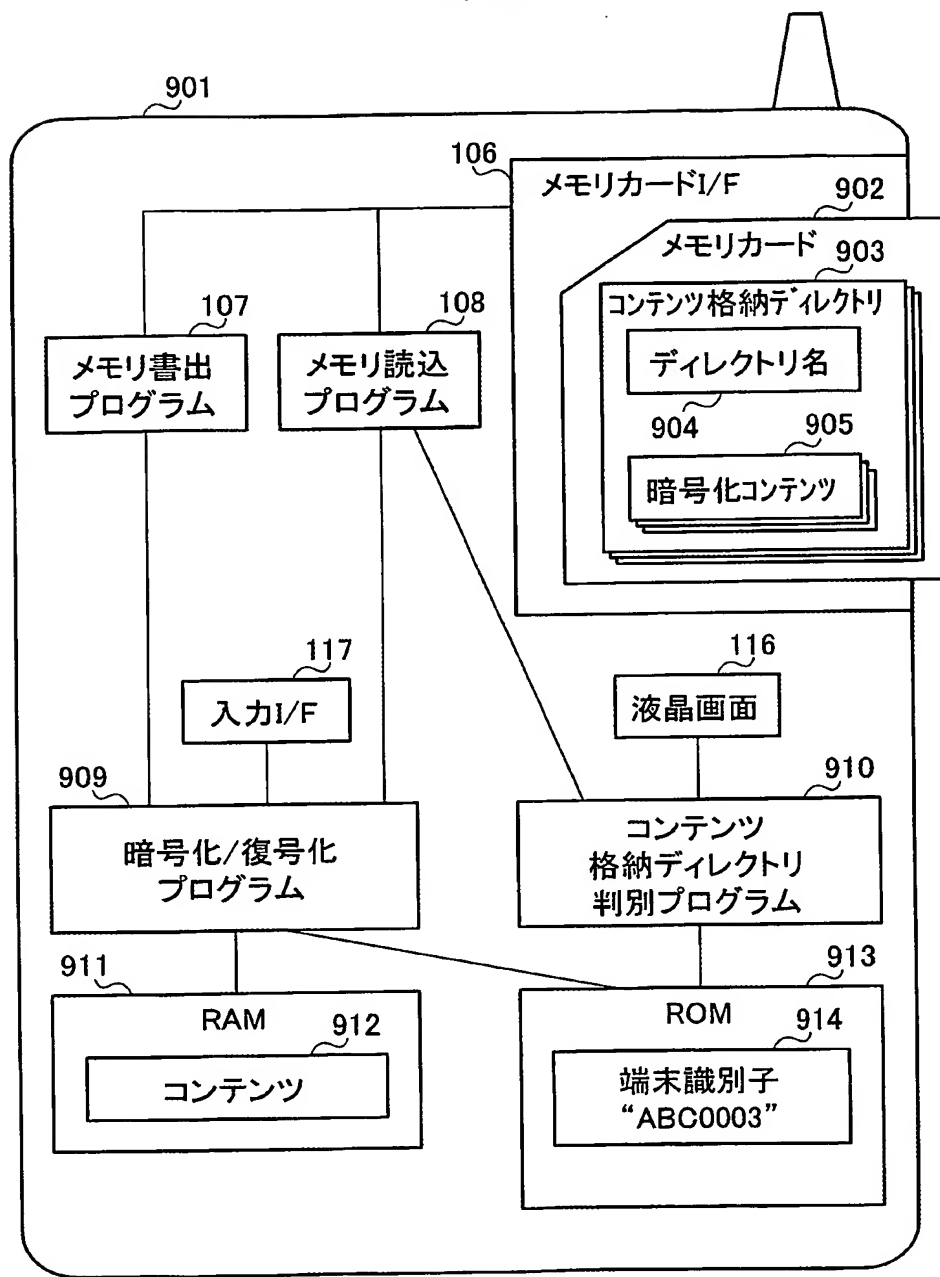


図 10

11/29

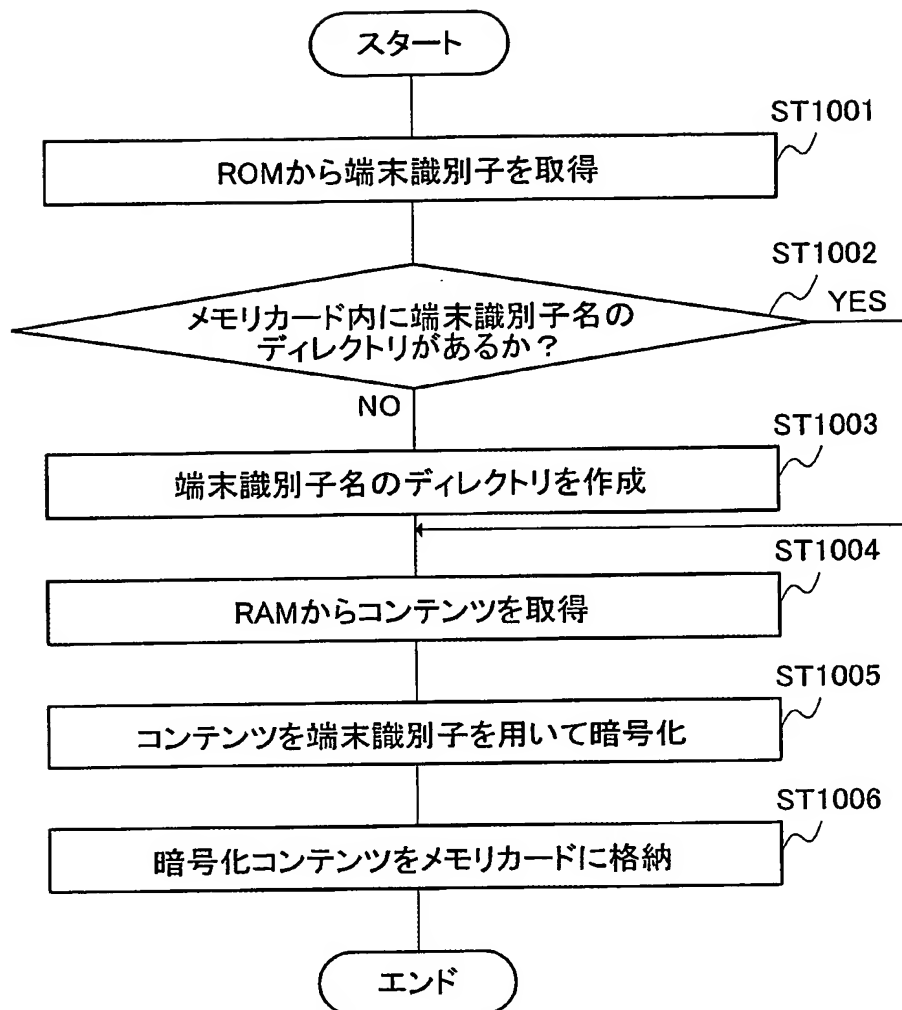


図 11

12/29

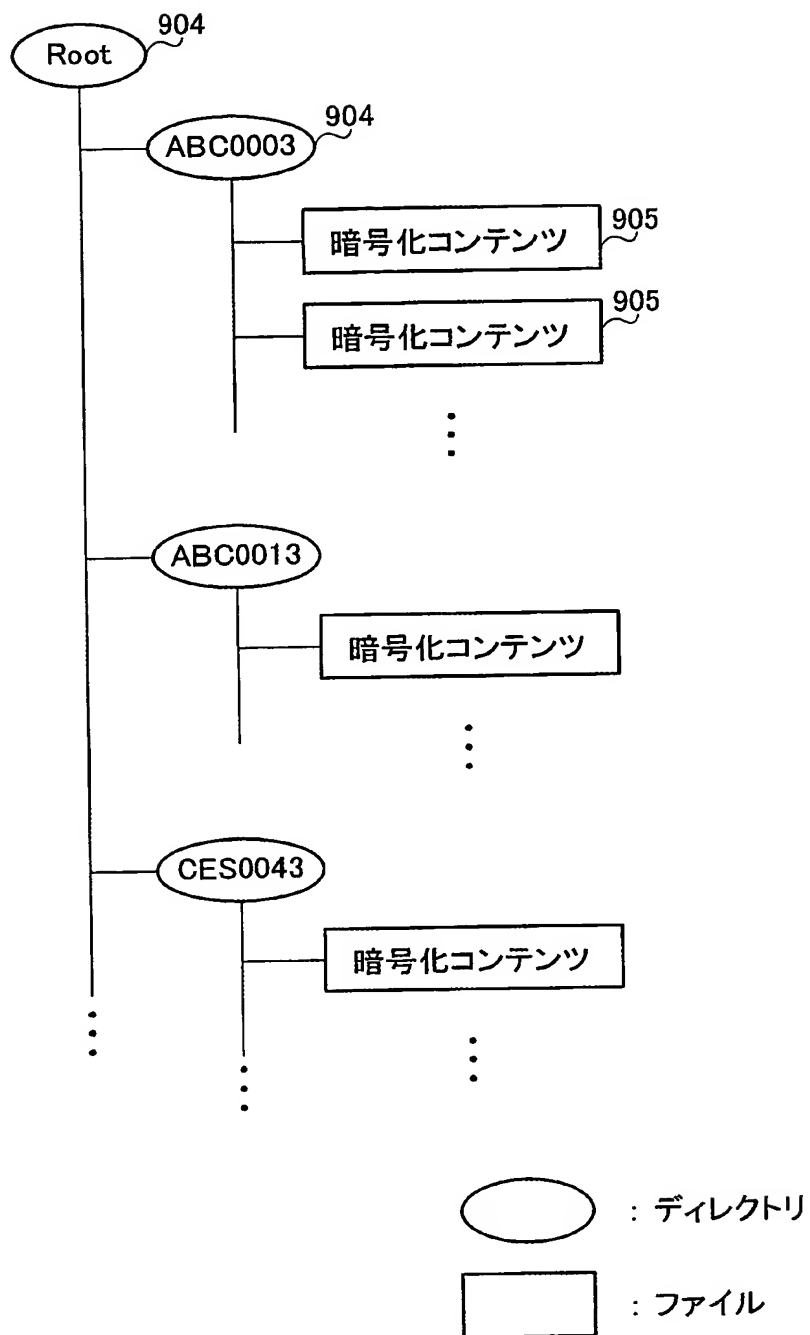


图 12

13/29

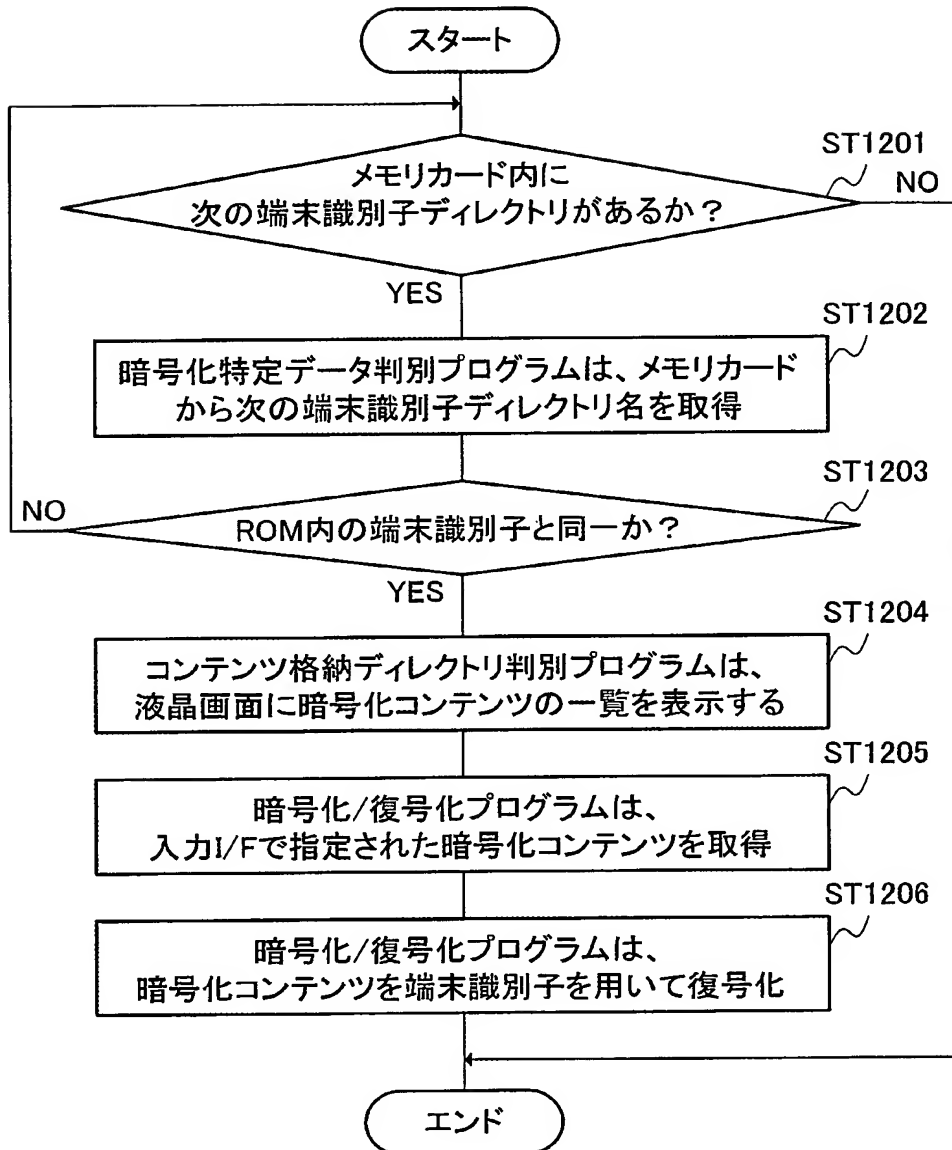


図 13

14/29

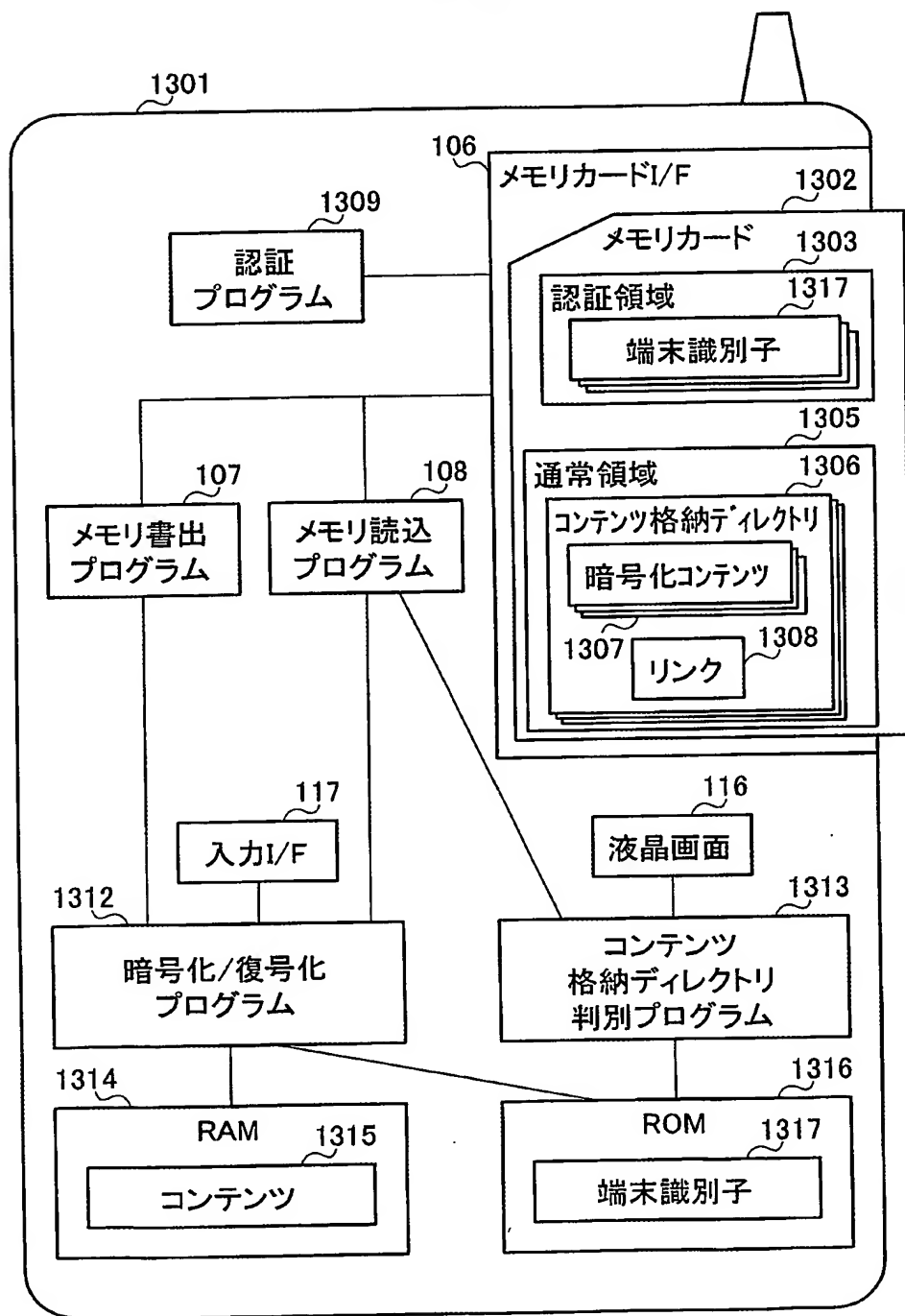


図 14

15/29

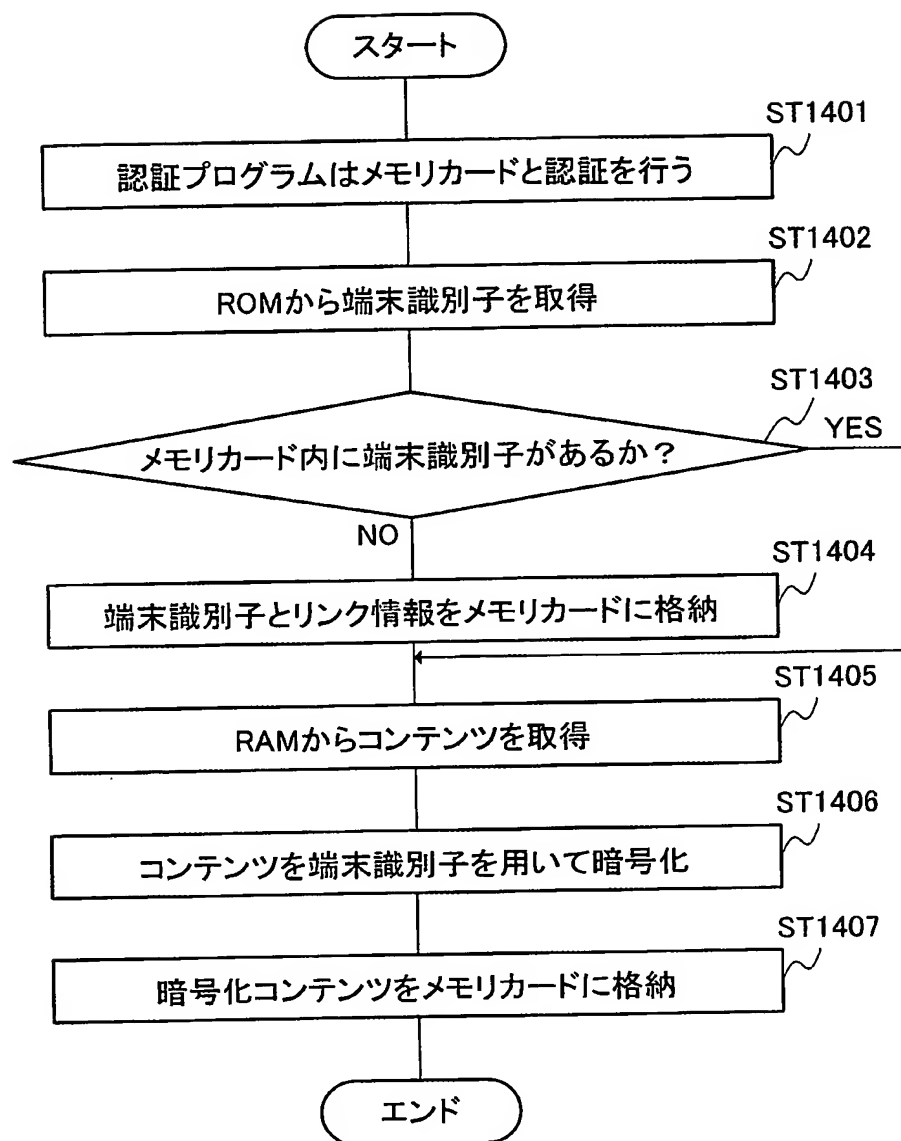


図 15

16/29

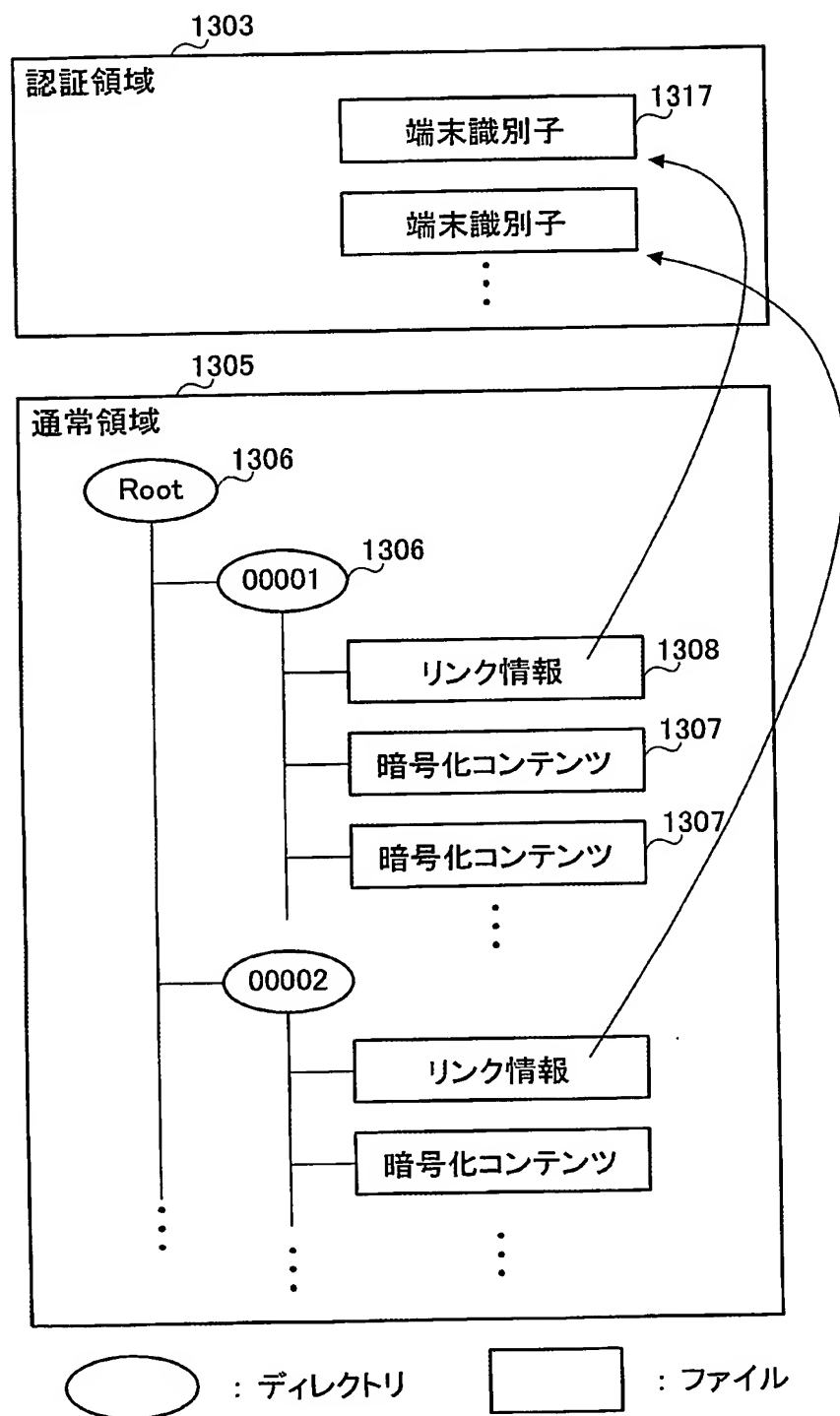


図 16

17/29

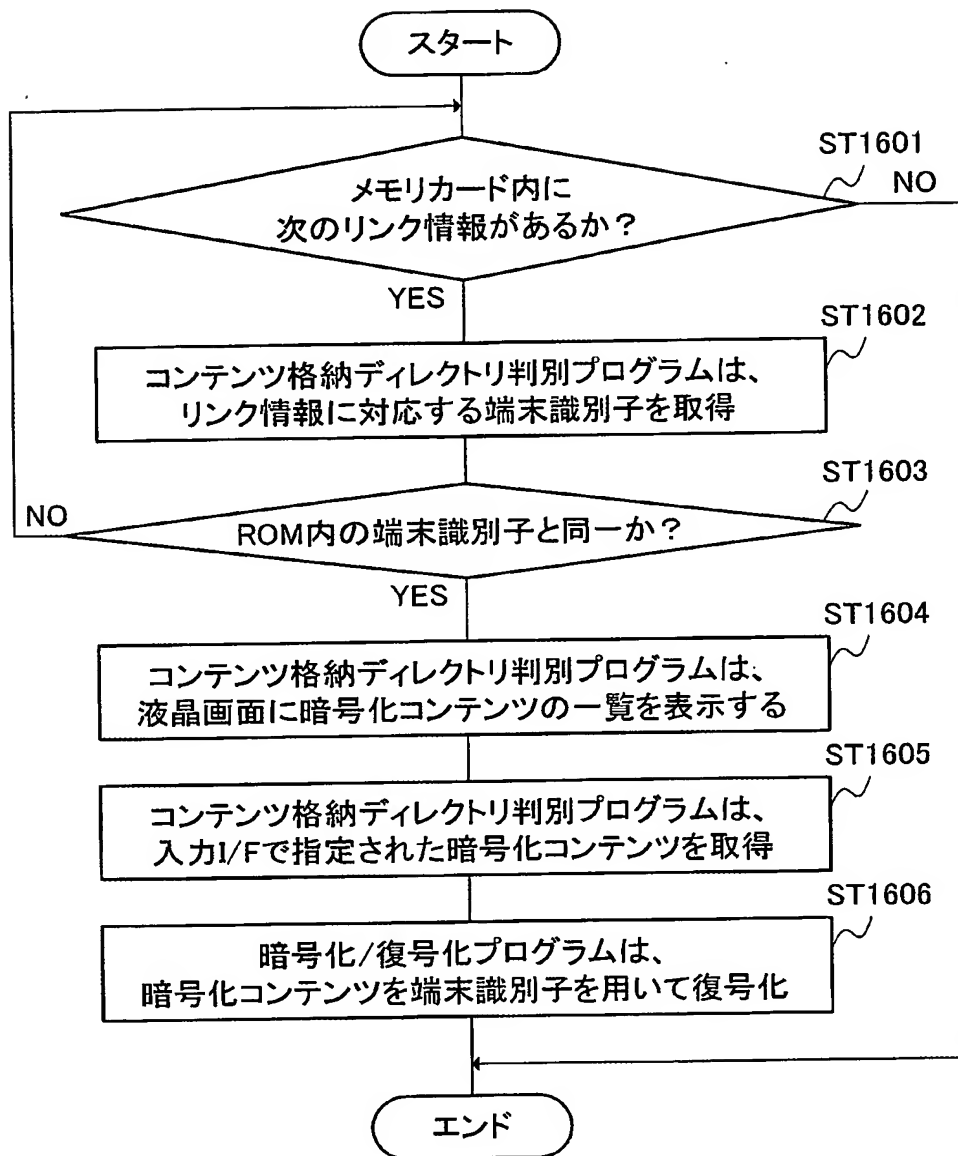


図 17

18/29

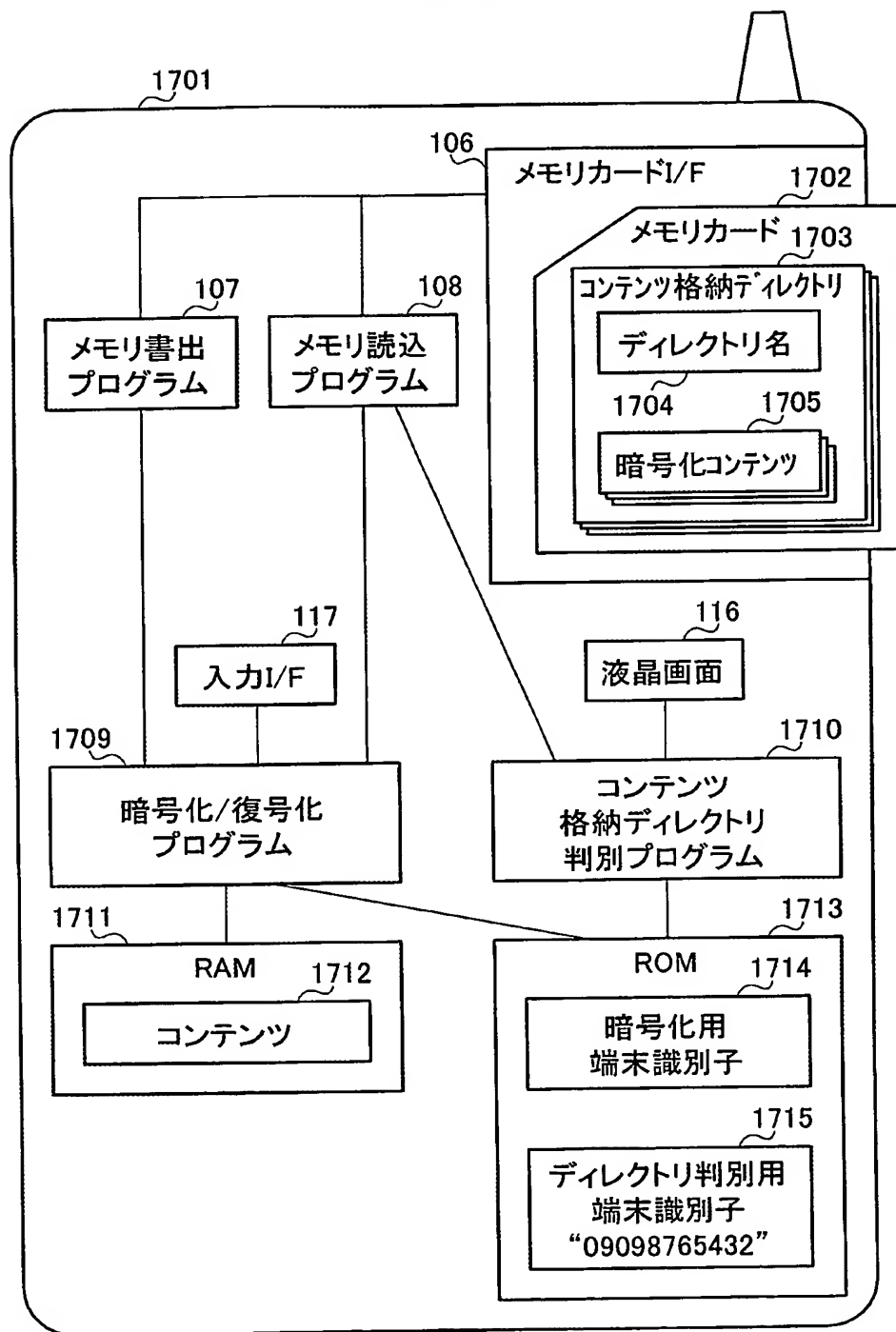


図 18

19/29

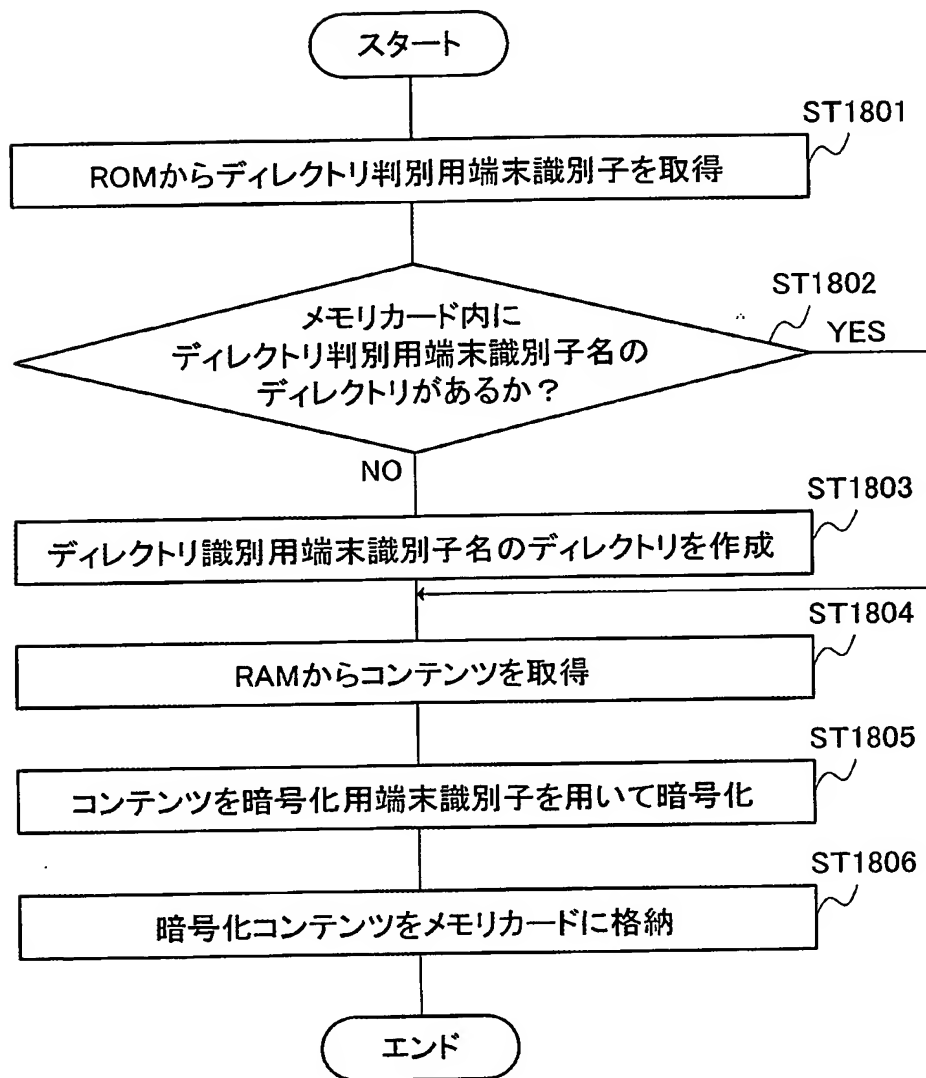


図 19

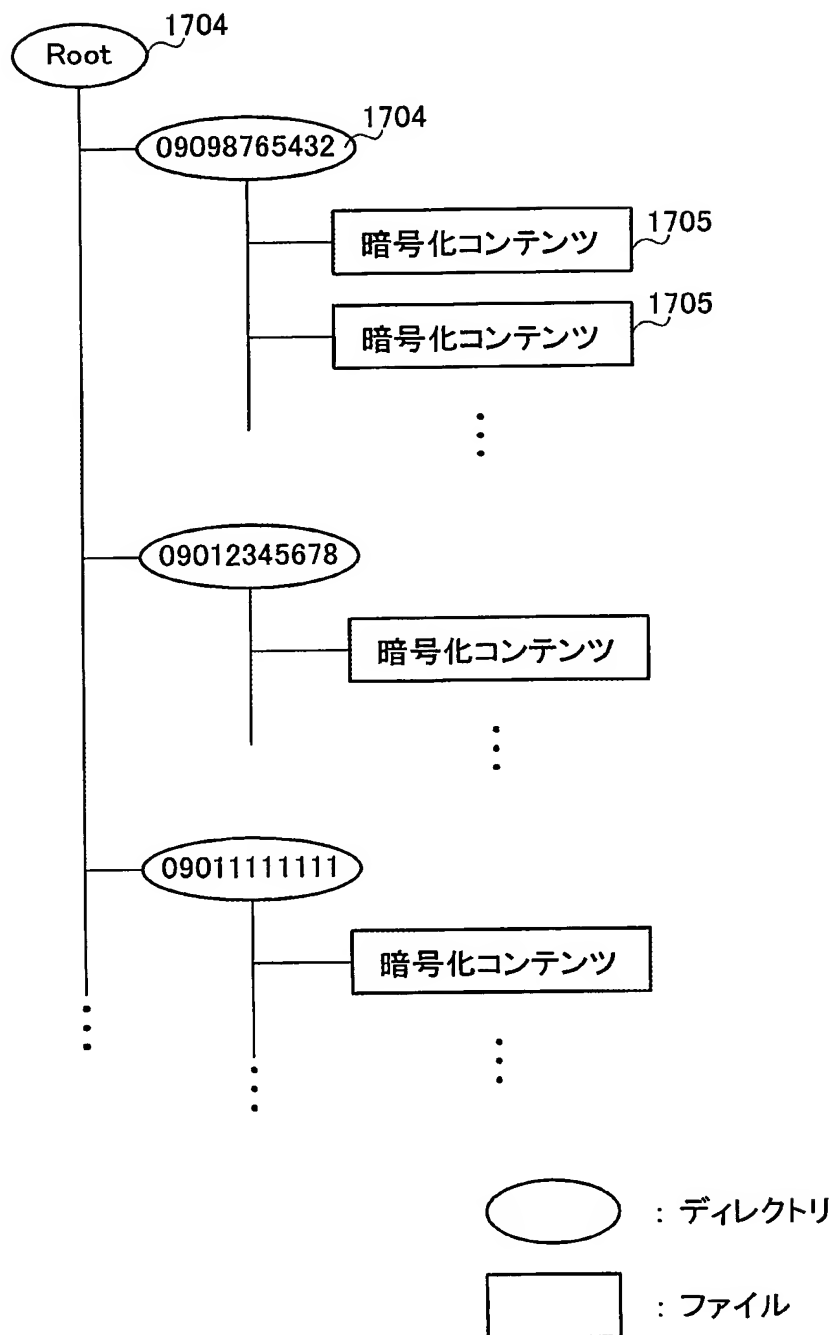


图 20

21/29

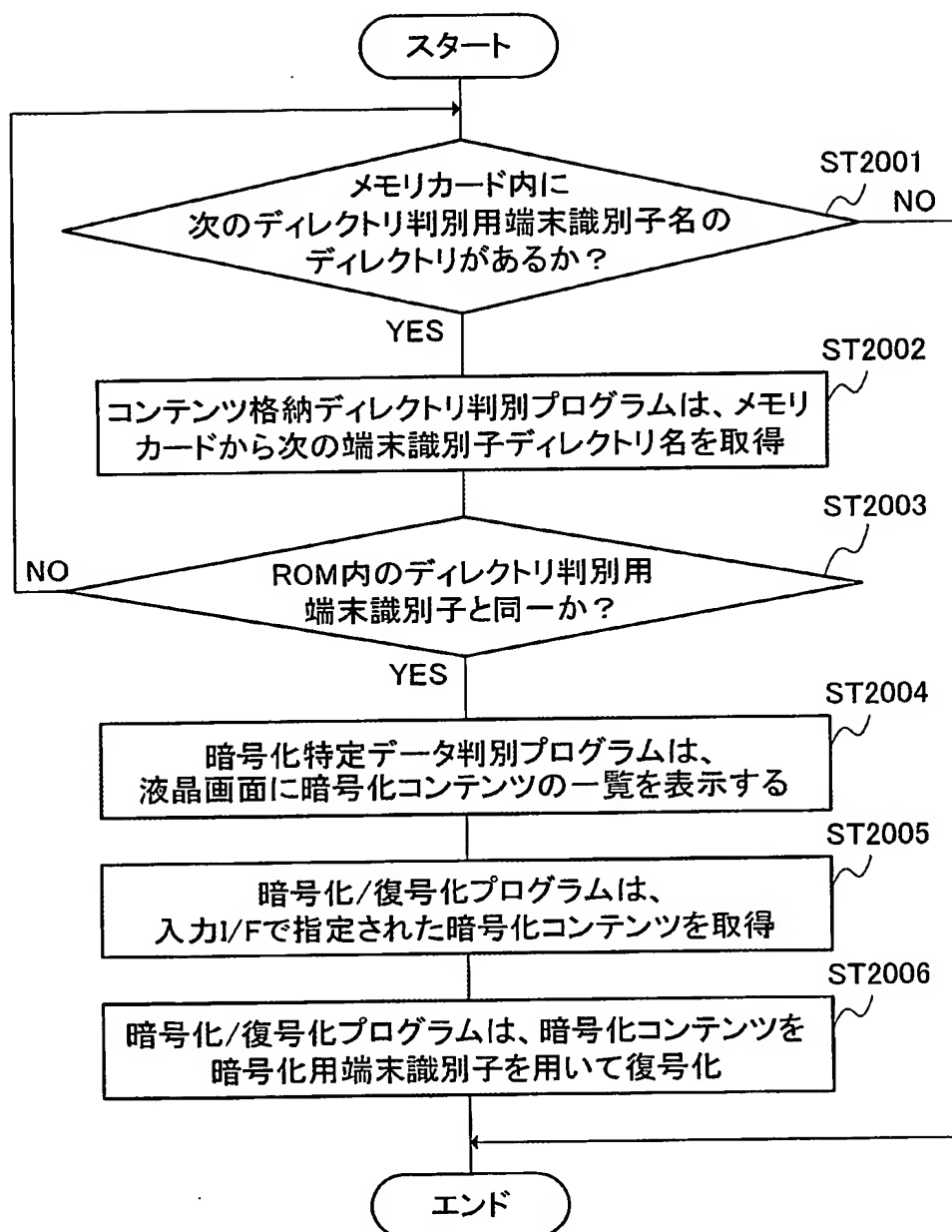


図 21

22/29

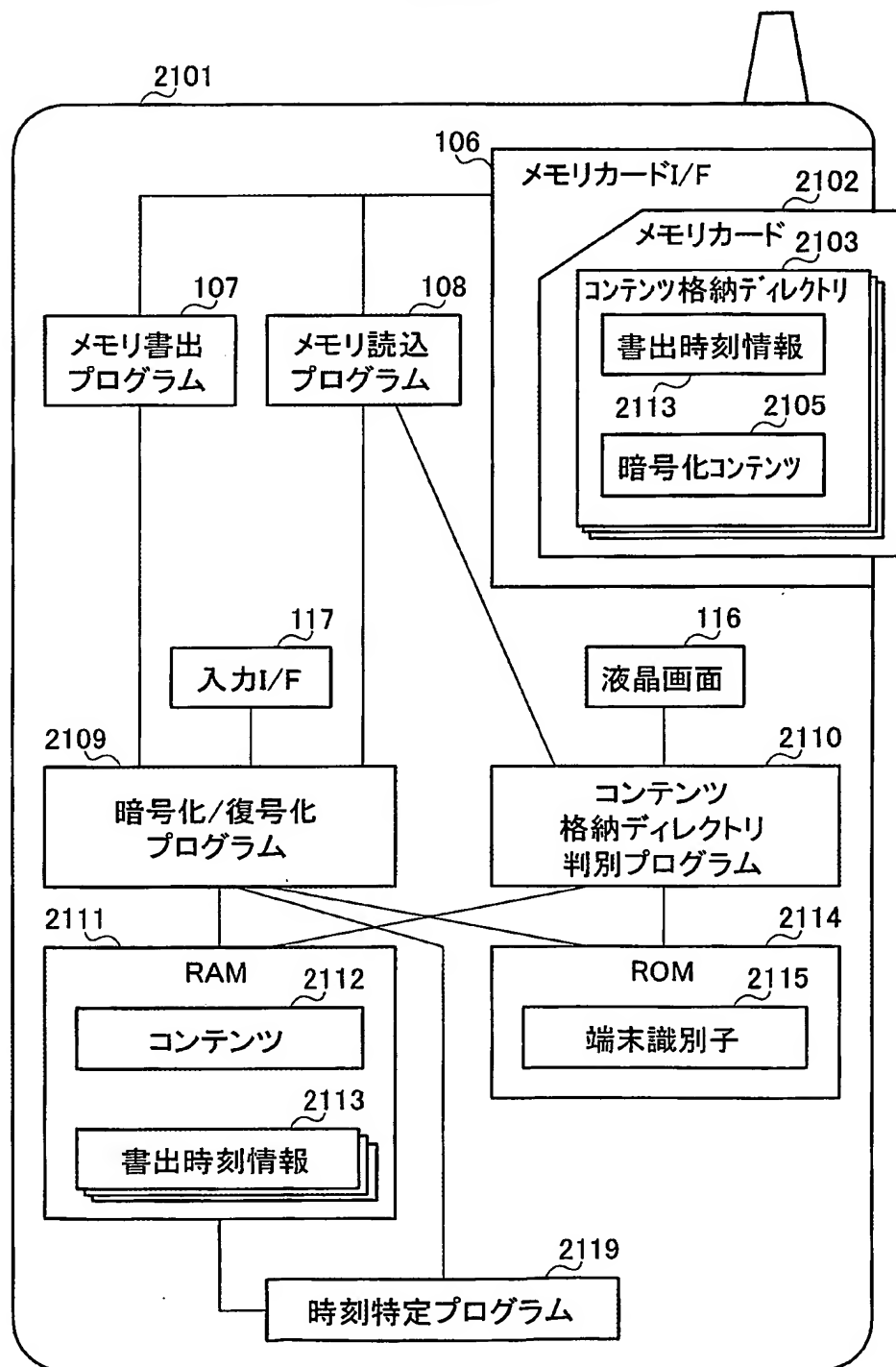


図 22

23/29

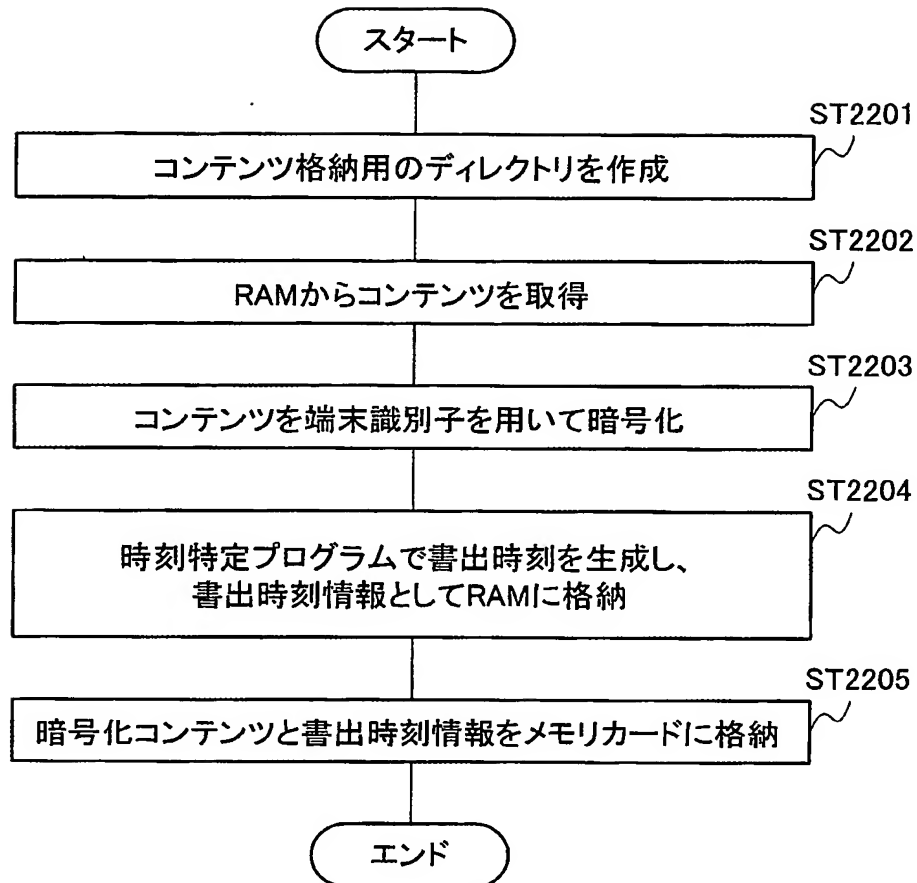


図 23

24/29

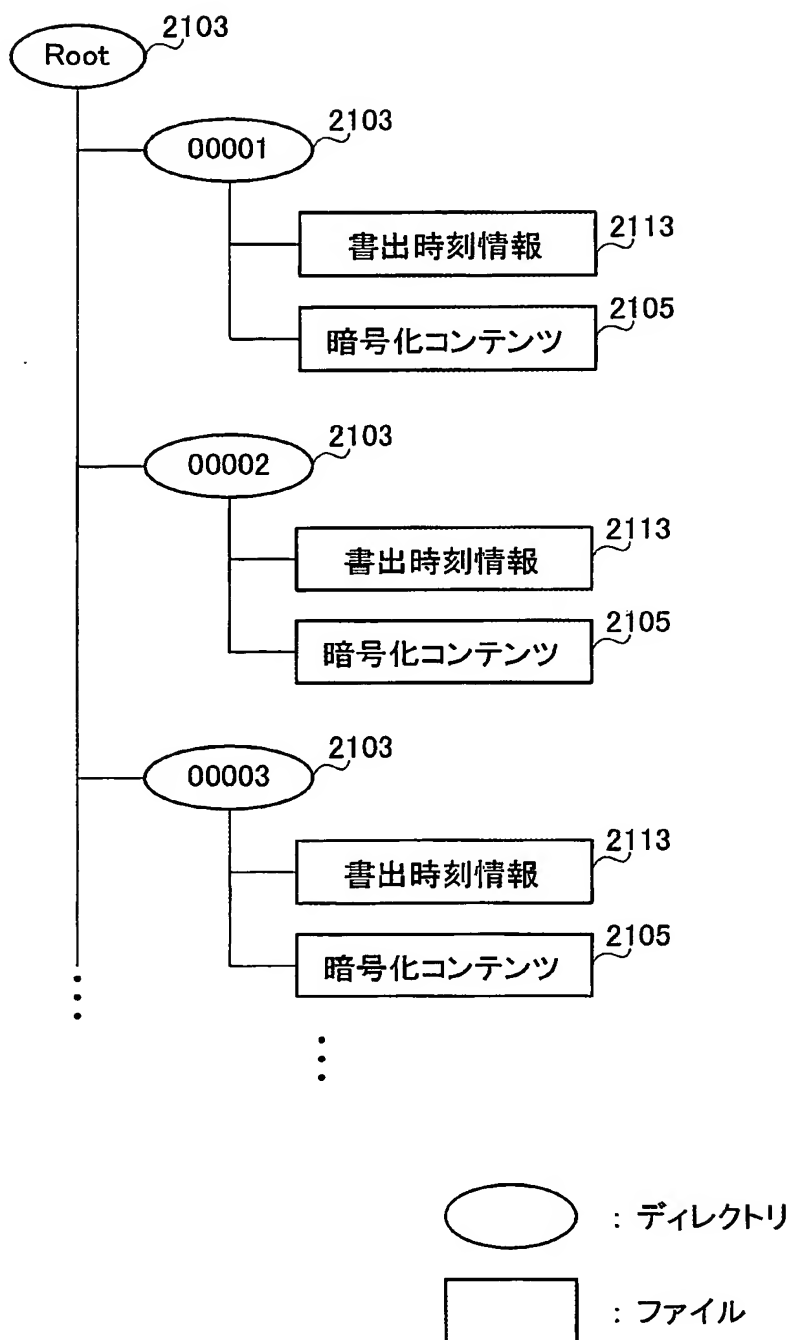


図 24

25/29

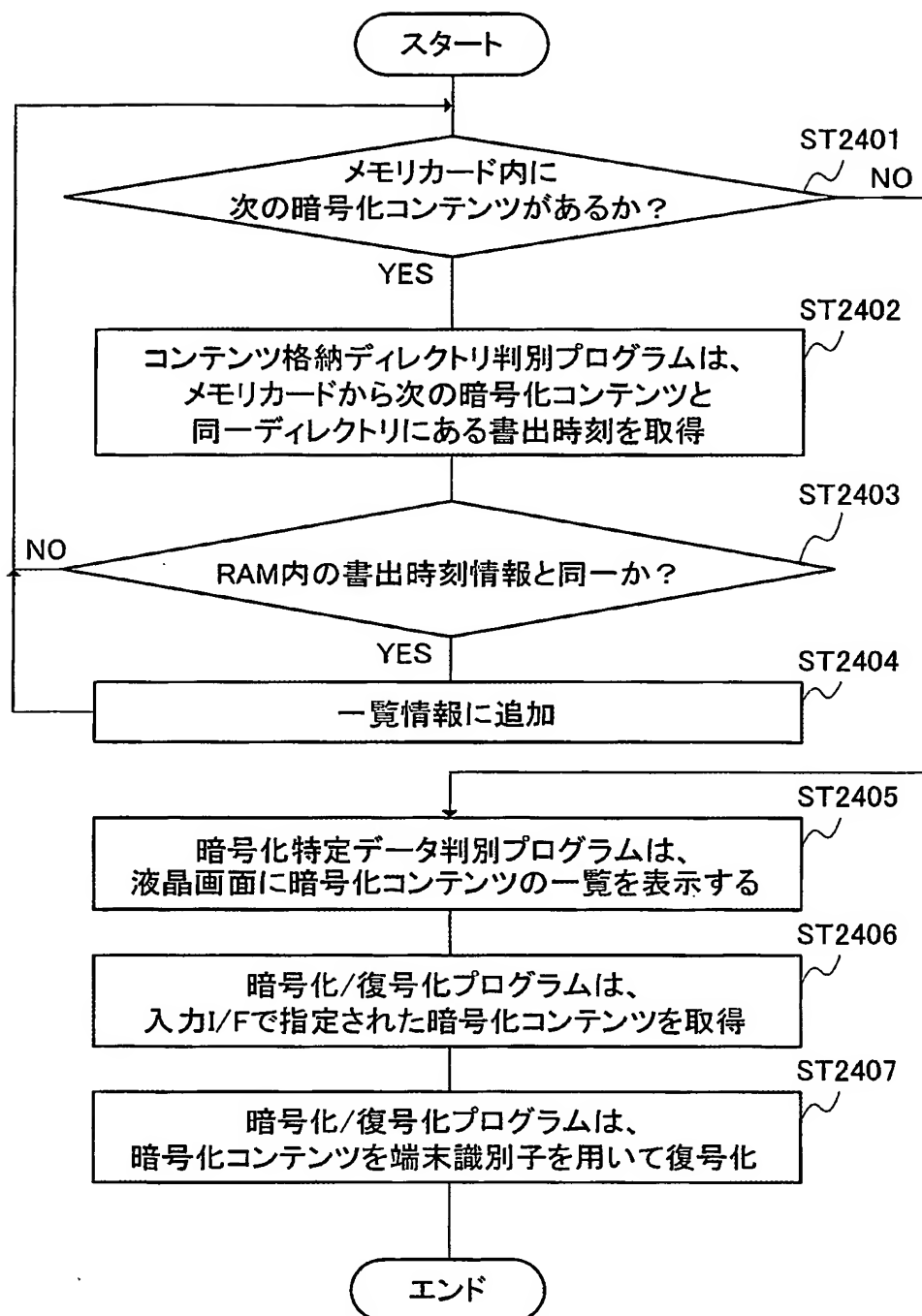


図 25

26/29

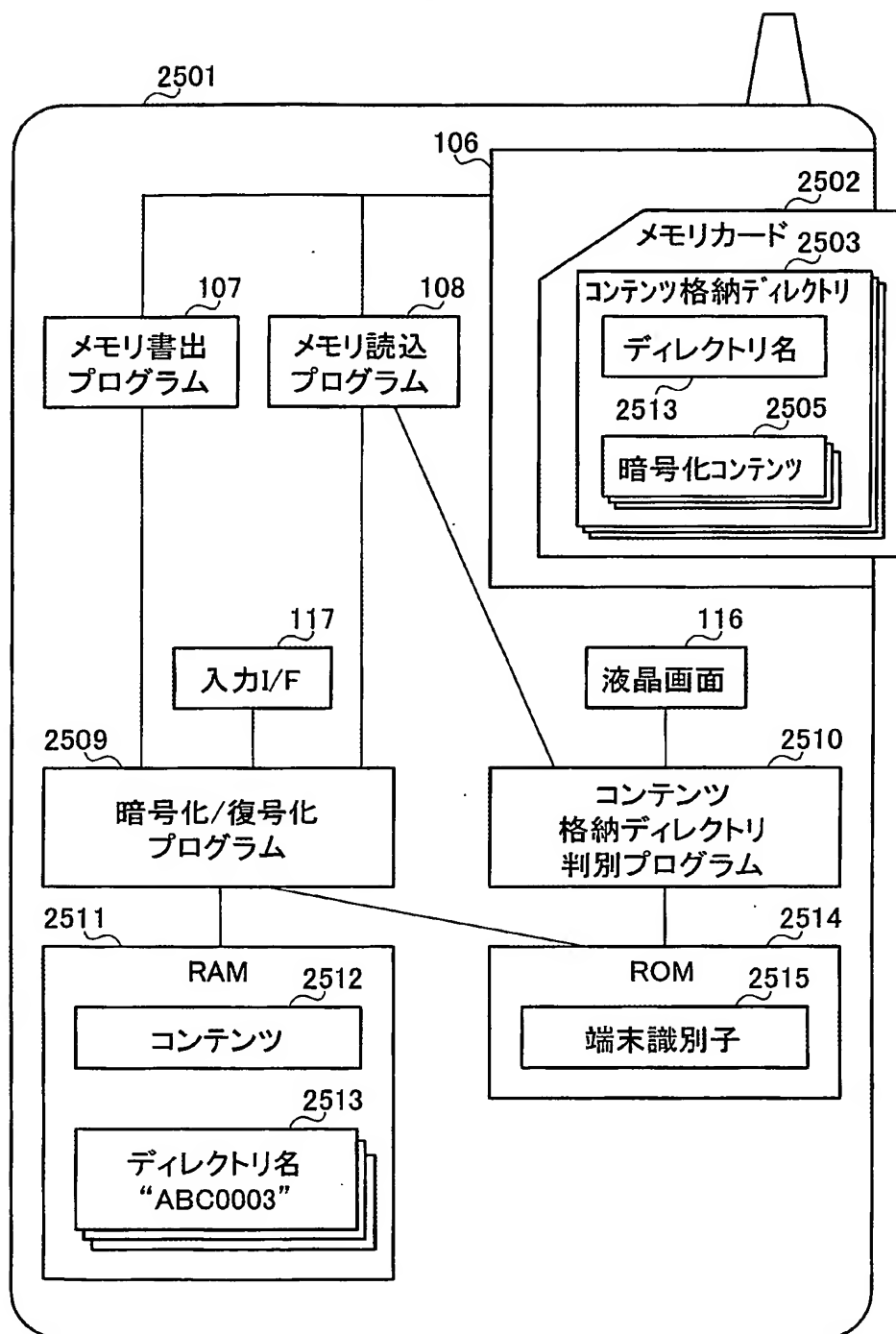


図 26

27/29

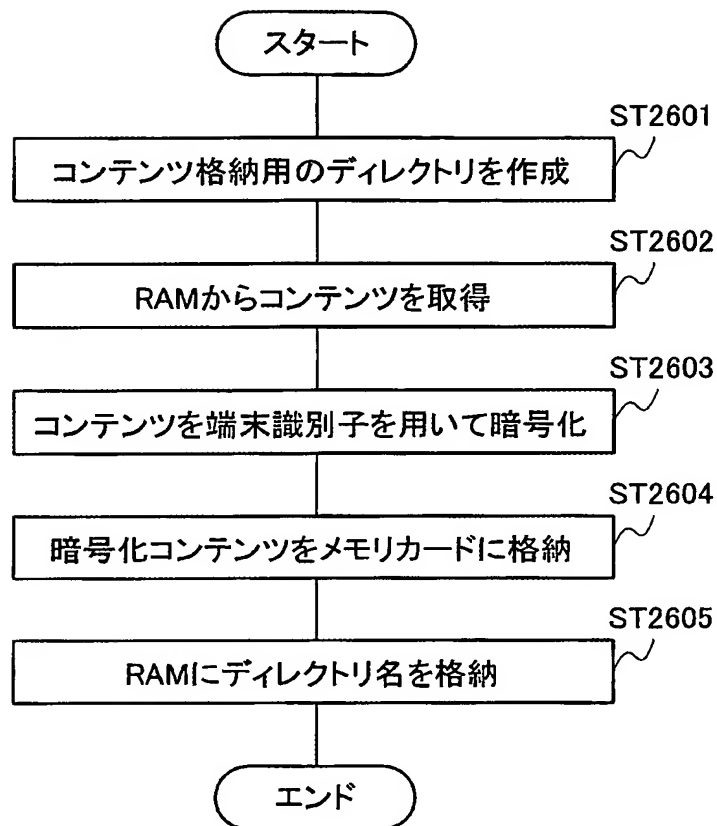


図 27

28/29

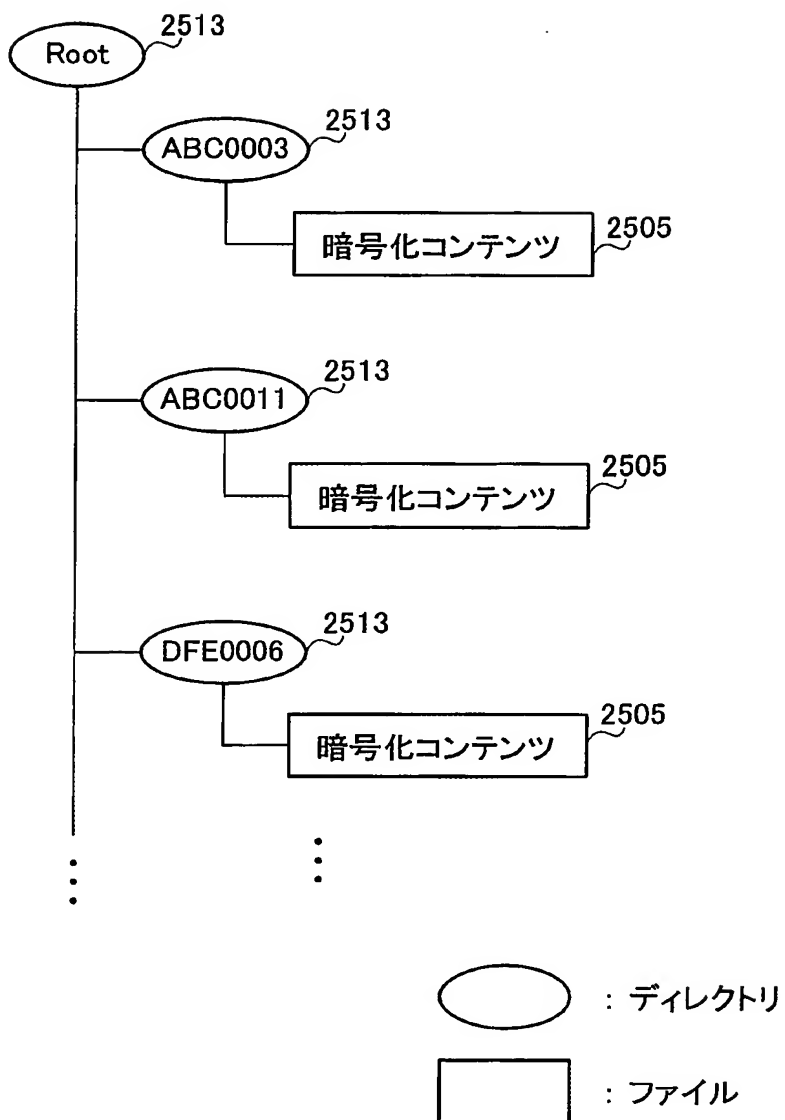


図 28

29/29

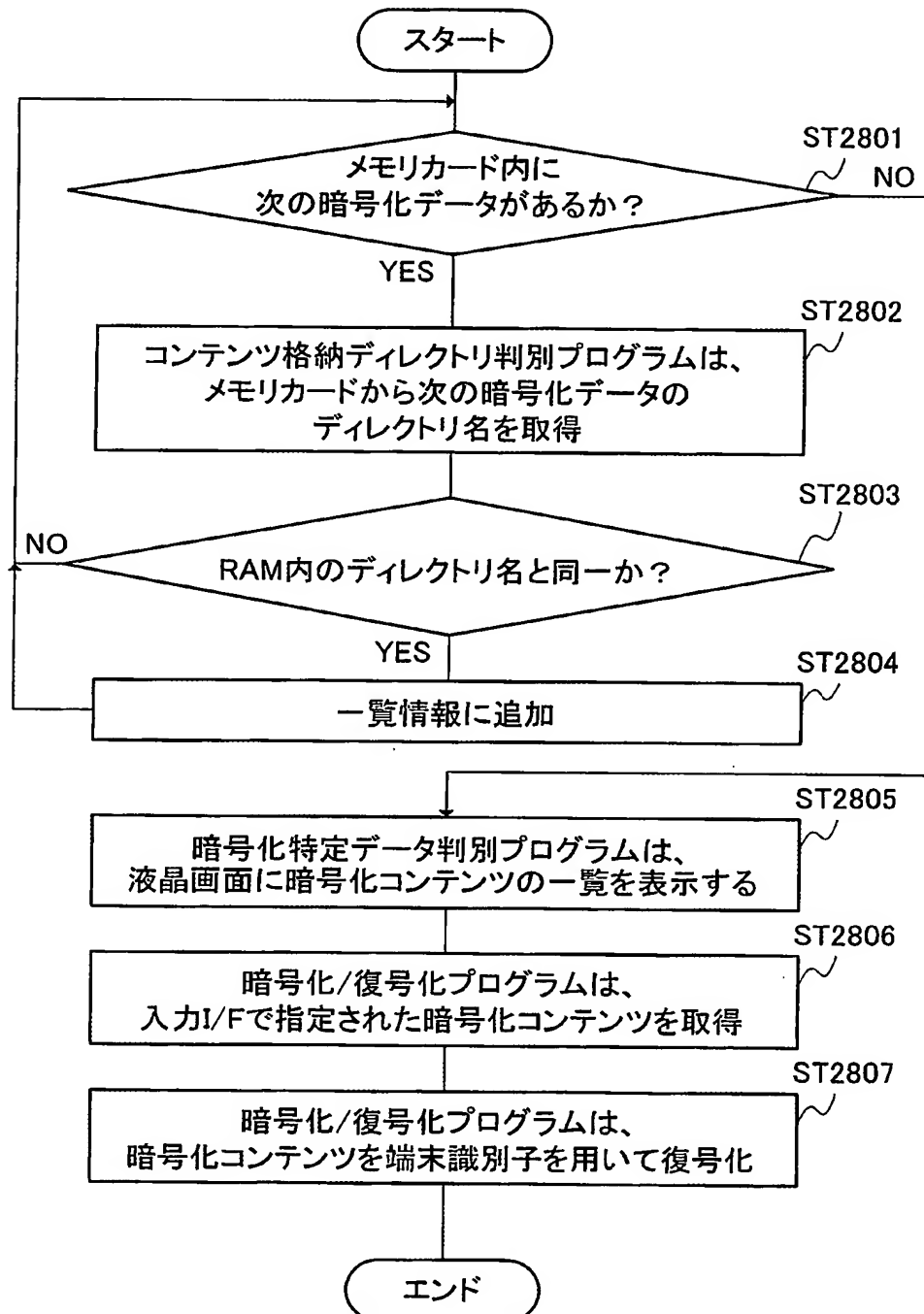


図 29

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/08 G11B20/10 G06F12/14 H04M11/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/08 G11B20/10 G06F12/14 H04M11/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
 日本国公開実用新案公報 1971-2003年
 日本国登録実用新案公報 1994-2003年
 日本国実用新案登録公報 1996-2003年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 2002-9966 A (ソフト流通株式会社) 2002. 01. 11, 全文, 図1-5 (ファミリーなし)	1-46
Y	JP 4-347949 A (株式会社東芝) 1992. 12. 03, 第【0048】-【0050】段落 & DE 69128981 C & EP 460538 A & US 5136642 A & EP 735723 A	1-46

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

12. 05. 03

国際調査報告の発送日

27.05.03

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

青木 重徳

5M

4229

電話番号 03-3581-1101 内線 3597

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 9-307543 A (松下電器産業株式会社) 1997. 11. 28, 全文, 図1-8 (ファミリーなし)	1-46